Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption*

Tatsuaki Okamoto
NTT
okamoto.tatsuaki@lab.ntt.co.jp

Katsuyuki Takashima
Mitsubishi Electric
Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

January 27, 2012

Abstract

This paper proposes the first inner product encryption (IPE) scheme that is adaptively secure and fully attribute-hiding (attribute-hiding in the sense of the definition by Katz, Sahai and Waters), while the existing IPE schemes are either fully attribute-hiding but selectively secure or adaptively secure but weakly attribute-hiding. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the decisional linear assumption in the standard model. The IPE scheme is comparably as efficient as the existing attribute-hiding IPE schemes. We also present a variant of the proposed IPE scheme with the same security that achieves shorter public and secret keys. A hierarchical IPE scheme can be constructed that is also adaptively secure and fully attribute-hiding under the same assumption. In this paper, we extend the dual system encryption technique by Waters into a more general manner, in which new forms of ciphertext and secret keys are employed and new types of information theoretical tricks are introduced along with several forms of computational reduction.

*This is the full version of a paper appearing in EUROCRYPT 2012, the 31st International Conference on the Theory and Applications of Cryptographic Techniques, April 15–19, 2012, Cambridge, United Kingdom.

Contents

1 Introduction

1.1 Background

Functional encryption (FE) is an advanced class of encryption and it covers identity-based encryption (IBE)[3, 4, 8, 14], hidden-vector encryption (HVE) [10], inner-product encryption (IPE) [19], predicate encryption (PE) and attribute-based encryption (ABE) [2, 17, 26, 20, 25, 27, 23]. In FE, there is a relation $R(v, x)$ which determines what a secret key with parameter v can decrypt a ciphertext encrypted under parameter x. The enhanced functionality and flexibility provided by FE systems are very appealing for many practical applications.

For some applications, the parameters for encryption are required to be hidden from ciphertexts. One of such applications is an advanced notion of PKE with keyword search (PEKS) [7], which we call *PKE with functional search* (PEFS) in this paper. In PEFS, a parameter x (not just a keyword) embedded in a ciphertext is searched (checked) whether $R(v, x)$ holds or not by using a secret key with parameter v. Here, keyword search is a special case of functional search $R(v, x)$ when $R(v, x) \Leftrightarrow [x = v]$. Parameter x of a ciphertext is often private information and should be hidden from ciphertexts in such applications.

To capture the security requirement, Katz, Sahai and Waters [19] introduced *attribute-hiding* (based on the same notion for HVE by Boneh and Waters [10]), a security notion for FE that is stronger than the basic security requirement, *payload-hiding*. Roughly speaking, attribute-hiding requires that a ciphertext conceal the associated parameter as well as the plaintext, while payload-hiding only requires that a ciphertext conceal the plaintext. Attribute-hiding FE is often called predicate encryption (PE).

The widest class of relations of a FE system in the literature is general non-monotone (span program) relations, which can be expressed using AND, OR, Threshold and NOT gates [23]. FE systems supporting such a wide class of relations, however, have one limitation in that the parameter x of the ciphertext should be revealed to users to decrypt. That is, such FE systems do not satisfy the attribute-hiding security.

To the best of our knowledge, the widest class of relations supported by attribute-hiding FE systems are *inner-product predicates* in [19, 20, 23], which we call the KSW08, LOS$^+$10 and OT10 schemes. Parameters of inner-product predicates are expressed as vectors $\vec{x}$ (for a ciphertext) and $\vec{v}$ (for a secret key), where $R(\vec{v}, \vec{x})$ holds iff $\vec{v} \cdot \vec{x} = 0$. (Here, $\vec{v} \cdot \vec{x}$ denotes the standard inner-product.) In this paper we call FE for inner-product predicates *inner product encryption* (IPE).

Inner-product predicates represent a fairly wide class of relations including equality tests as the simplest case (i.e., anonymous IBE and HVE are very special classes of attribute-hiding IPE), disjunctions or conjunctions of equality tests, and, more generally, CNF or DNF formulas. We note, however, that inner product predicates are less expressive than general (even monotone span program) relations of FE. To use inner product predicates for such general relations, formulas must be written in CNF or DNF form, which can cause a super-polynomial blowup in size for arbitrary formulas.

Among the existing attribute-hiding IPEs, the KSW08 IPE scheme [19] is proven to be only *selectively* secure. Although the LOS$^+$10 and OT10 IPE schemes [20, 23] are proven to be *adaptively* secure, the achieved attribute-hiding security is limited or weaker than that defined in [19]. Here, we call the attribute-hiding security defined in [19] *fully attribute-hiding* and that achieved in [20, 23] *weakly attribute-hiding*. In the fully attribute-hiding security definition [19], adversary $\mathcal{A}$ is allowed to ask a key-query for $\vec{v}$ such that $\vec{v} \cdot \vec{x}^{(0)} = \vec{v} \cdot \vec{x}^{(1)} = 0$ provided that $m^{(0)} = m^{(1)}$ ($\vec{x}^{(b)}$ and $m^{(b)}$ ($b = 0, 1$) are for the challenge ciphertext in the security definition), while in the weakly attribute-hiding security definition [20, 23], $\mathcal{A}$ is only allowed to ask a key-query for $\vec{v}$ such that $\vec{v} \cdot \vec{x}^{(b)} \neq 0$ for all $b \in \{0, 1\}$.

Let us explain the difference between the fully and weakly attribute-hiding definitions in a PEFS system. User Alice provides her secret key, $\mathsf{sk}_{\vec{v}}$, to proxy server Bob, who checks whether $\vec{v} \cdot \vec{x} = 0$ or not for an incoming ciphertext, $\mathsf{ct}_{\vec{x}}$, encrypted with parameter $\vec{x}$. In the weakly attribute-hiding security, privacy of $\vec{x}$ from $\mathsf{ct}_{\vec{x}}$ is ensured only if $\vec{v} \cdot \vec{x} \neq 0$, but cannot be ensured or some privacy on $\vec{x}$ may be revealed if $\vec{v} \cdot \vec{x} = 0$. Here note that there still exists $(n-1)$-dimensional freedom (or room of privacy) of n-dimensional vector $\vec{x}$, even if $\vec{v}$ and the fact that $\vec{v} \cdot \vec{x} = 0$ is revealed. For example, let $\vec{v}$ express formula on an email message attributes, [[Subject $= X$] $\vee$ [Subject $= Y$]] $\wedge$ [[Receiver = Alice] $\vee$ [Receiver = Alice's secretary]], and $\vec{x}$ express ciphertext attribute (Subject $= X$, Receiver = Alice). In this case, $\vec{v} \cdot \vec{x} = 0$, since the

ciphertext attribute expressed by $\vec{x}$ satisfies the formula expressed by $\vec{v}$. Although Bob knows $\mathsf{sk}_{\vec{v}}$ and $\vec{v}$, Bob has no idea which attribute $\vec{x}$ is embedded in $\mathsf{ct}_{\vec{x}}$ except that the ciphertext attribute satisfies the formula, i.e., $\vec{v}\cdot\vec{x}=0$, if the fully attribute-hiding security is achieved. On the other hand, Bob may obtain some additional information on the attribute (e.g., Bob may know that the subject is X, not Y), if only the weakly attribute-hiding security is guaranteed.

The KSW08 IPE scheme is fully attribute-hiding but selectively secure, and the LOS$^+$10 and OT10 IPE schemes are adaptively secure but weakly attribute-hiding. Therefore, there is no IPE scheme that is adaptively secure and fully attribute-hiding simultaneously. As for a more limited class of schemes, HVE (as mentioned above, HVE is a very special class of attribute-hiding IPE), an adaptively secure and fully attribute-hiding HVE scheme has been proposed [13]. For hierarchical IPE (HIPE), the LOS$^+$10 and OT10 HIPE schemes [20, 23] are adaptively secure but weakly attribute-hiding, i.e., there is no HIPE scheme that is adaptively secure and fully attribute-hiding simultaneously.

It is a technically challenging task to achieve an adaptively secure and fully attribute-hiding (H)IPE scheme. Even if we use the powerful dual system encryption technique by Waters, the main difficulty resides in how to change a (normal) secret key queried with $\vec{v}$ to a semi-functional secret key, without knowing $\vec{x}^{(b)}$ $(b=0,1)$ for the challenge ciphertext, i.e., without knowing whether $\vec{v}\cdot\vec{x}^{(b)}=0$ or not, since an adversary may issue key queries with $\vec{v}$ before issuing the challenge ciphertext query with $\vec{x}^{(b)}$ $(b=0,1)$ and two possible cases, $\vec{v}\cdot\vec{x}^{(b)}=0$ (for all $b\in\{0,1\}$) and $\vec{v}\cdot\vec{x}^{(b)}\neq 0$ (for all $b\in\{0,1\}$), are allowed in *fully* attribute-hiding IPE. Note that in *weakly* attribute-hiding IPE, it is always required that $\vec{v}\cdot\vec{x}^{(b)}\neq 0$. At a first glance, it looks hard to achieve it, since the form of semi-functional secret key may be different (e.g., canceled or randomized) depending on whether $\vec{v}\cdot\vec{x}^{(b)}=0$ or not. Another technically challenging target in this paper is to prove the security under the decisional linear (DLIN) assumption (on prime order pairing groups) in the standard model.

1.2 Our Results

This paper proposes the first IPE scheme that is adaptively secure and fully attribute-hiding simultaneously. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the DLIN assumption in the standard model (Section 4). We also present a variant of the proposed IPE scheme with the same security that achieves shorter master public keys and shorter secret keys (Section 5). A hierarchical IPE (HIPE) scheme can be realized that is also adaptively secure and fully attribute-hiding under the same assumption. Table 2 in Section 6 compares the proposed IPE schemes with several existing attribute-hiding IPE schemes.

1.3 Key Techniques

To overcome the above-mentioned difficulty, we extend the dual system encryption technique into a more general manner, in which various forms of ciphertext and secret keys are introduced ('normal', 'temporal 0', 'temporal 1', 'temporal 2' and 'unbiased' forms for a ciphertext, and 'normal', 'temporal 1' and 'temporal 2' forms for a secret key), and new types (Types 1, 2, 3) of information theoretical tricks are employed with several forms of computational reduction (the security of Problems 1, 2 and 3 to DLIN). See Table 1 and Figure 1 in Section 4.3.2 for the outline.

In our approach, all forms ('normal', 'temporal 1' and 'temporal 2') of a secret key do not depend on whether $\vec{v}\cdot\vec{x}^{(b)}=0$ or not. Although the aim of a 'semi-functional' secret key in the original dual system encryption method is to randomize the semi-functional part, the aim of these forms of a secret-key in our approach is just to encode $\vec{v}$ in a (hidden) subspace for a secret-key.

Another key point in our approach is that we transform a challenge ciphertext to an 'unbiased' ciphertext whose advantage is 0 in the final game, and $\vec{x}^{(b)}$ is randomized to a random vector in a two-dimensional subspace, $\mathsf{span}\langle\vec{x}^{(0)}, \vec{x}^{(1)}\rangle$. In contrast, $\vec{x}^{(b)}$ is randomized to a random vector in the n-dimensional whole space, $\mathbb{F}_q^n$, in [20, 23] for weakly attribute-hiding IPE based on the original dual system encryption technique.

Therefore, in our approach, only $\vec{v}$ is encoded in a (hidden) subspace of the temporal forms of a secret-key, and a random vector in $\mathsf{span}\langle\vec{x}^{(0)}, \vec{x}^{(1)}\rangle$ is encoded in the corresponding (hidden) subspace for the temporal and unbiased forms of a ciphertext.

To realize this approach, our construction is based on the dual pairing vector spaces (DPVS) (Section 2) [20, 23]. A nice property of DPVS is that we can set a hidden linear subspace by concealing the basis of a subspace from the public key. Typically, a pair of dual (or orthonormal) bases, $\mathbb{B}$ and $\mathbb{B}^*$, are randomly generated using random linear transformation, and a part of $\mathbb{B}$ (say $\hat{\mathbb{B}}$) is used as a public key and the corresponding part of $\mathbb{B}^*$ (say $\hat{\mathbb{B}}^*$) is used as a secret key or trapdoor. Therefore, the basis, $\mathbb{B} - \hat{\mathbb{B}}$, is information theoretically concealed against an adversary, i.e., even an infinite power adversary has no idea on which basis is selected as $\mathbb{B} - \hat{\mathbb{B}}$ when $\hat{\mathbb{B}}$ is published. It provides a framework for information theoretical tricks in the public-key setting.

In the proposed (basic) IPE scheme, $\mathsf{span}\langle\mathbb{B}\rangle$ and $\mathsf{span}\langle\mathbb{B}^*\rangle$, are $(4n+2)$-dimensional (where the dimension of inner-product vectors is n), and, as for public parameter $\hat{\mathbb{B}}$, $\mathsf{span}\langle\hat{\mathbb{B}}\rangle$ is $(2n+2)$-dimensional, i.e., the basis for the remaining $2n$-dimensional space is information theoretically concealed (ambiguous). We use the $2n$-dimensional hidden subspace to realize the various forms of ciphertext and secret keys and make elaborate game transformations over these forms towards the final goal, the 'unbiased' ciphertext.

The game transformations are alternating over computational and conceptual (information theoretical), and the combinations of three types of information theoretical tricks and three computational tricks (Problems 1, 2 and 3) play a central role in our approach, as shown in Figure 1. Type 1 is a (conceptual) linear transformation inside a (hidden) subspace for a ciphertext, Type 2 is a (conceptual) linear transformation inside a (hidden) subspace for a ciphertext with preserving the corresponding secret key value, and Type 3 is a (conceptual) linear transformation across (hidden and partially public) subspaces. The security of Problems 1, 2 and 3 is reduced to the DLIN assumption.

See Section 4.3.2 for the details of our techniques, in which the game transformations as well as the form changes of ciphertext and secret keys are summarized in Table 1 and Figure 1.

1.4 Notations

When A is a random variable or distribution, $y \xleftarrow{\mathsf{R}} A$ denotes that y is randomly selected from A according to its distribution. When A is a set, $y \xleftarrow{\mathsf{U}} A$ denotes that y is uniformly selected from A. $y := z$ denotes that y is set, defined or substituted by z. When a is a fixed value, $A(x) \to a$ (e.g., $A(x) \to 1$) denotes the event that machine (algorithm) A outputs a on input x. A function $f : \mathbb{N} \to \mathbb{R}$ is *negligible* in λ, if for every constant $c > 0$, there exists an integer n such that $f(\lambda) < \lambda^{-c}$ for all $\lambda > n$.

We denote the finite field of order q by $\mathbb{F}_q$, and $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^\times$. A vector symbol denotes a vector representation over $\mathbb{F}_q$, e.g., $\vec{x}$ denotes $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. For two vectors $\vec{v} = (v_1, \ldots, v_n)$ and $\vec{x} = (x_1, \ldots, x_n)$, $\vec{v} \cdot \vec{x}$ denotes the inner-product $\sum_{i=1}^n x_i v_i$. The vector $\vec{0}$ is abused as the zero vector in $\mathbb{F}_q^n$ for any n. X^{T} denotes the transpose of matrix X. I_ℓ denotes the $\ell \times \ell$ identity matrix. A bold face letter denotes an element of vector space $\mathbb{V}$, e.g., $\boldsymbol{x} \in \mathbb{V}$. When $\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$, $\mathsf{span}\langle\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\rangle \subseteq \mathbb{V}$ (resp. $\mathsf{span}\langle\vec{x}_1, \ldots, \vec{x}_n\rangle$) denotes the subspace generated by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ (resp. $\vec{x}_1, \ldots, \vec{x}_n$). For bases $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ and $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$,

$(x_1,\ldots,x_N)_{\mathbb{B}} := \sum_{i=1}^N x_i \boldsymbol{b}_i$ and $(v_1,\ldots,v_N)_{\mathbb{B}^*} := \sum_{i=1}^N v_i \boldsymbol{b}_i^*$. $GL(n,\mathbb{F}_q)$ denotes the general linear group of degree n over $\mathbb{F}_q$.

2 Dual Pairing Vector Spaces (DPVS) and the Decisional Linear (DLIN) Assumption

Definition 1 *"Symmetric bilinear pairing groups"* $(q,\mathbb{G},\mathbb{G}_T,G,e)$ *are a tuple of a prime* q*, cyclic additive group* $\mathbb{G}$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G \neq 0 \in \mathbb{G}$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$ *i.e.,* $e(sG,tG) = e(G,G)^{st}$ *and* $e(G,G) \neq 1$*. Let* $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $(q,\mathbb{G},\mathbb{G}_T,\ G,e)$ *with security parameter* λ*.*

In this paper, we concentrate on the symmetric version of dual pairing vector spaces [21, 22]. constructed by using symmetric bilinear pairing groups given in Definition 1. For the asymmetric version of DPVS, $(q,\mathbb{V},\mathbb{V}^*,\mathbb{G}_T,\mathbb{A},\mathbb{A}^*,e)$, see Appendix A.2. The following symmetric version is obtained by identifying $\mathbb{V}=\mathbb{V}^*$ and $\mathbb{A}=\mathbb{A}^*$ in the asymmetric version.

Definition 2 *"Dual pairing vector spaces (DPVS)"* $(q,\mathbb{V},\mathbb{G}_T,\mathbb{A},e)$ *by a direct product of symmetric pairing groups* $(q,\mathbb{G},\mathbb{G}_T,G,e)$ *are a tuple of prime* q*,* N*-dimensional vector space* $\mathbb{V} := \overbrace{\mathbb{G}\times\cdots\times\mathbb{G}}^{N}$ *over* $\mathbb{F}_q$*, cyclic group* $\mathbb{G}_T$ *of order* q*, canonical basis* $\mathbb{A} := (\boldsymbol{a}_1,\ldots,\boldsymbol{a}_N)$ *of* $\mathbb{V}$*, where* $\boldsymbol{a}_i := (\overbrace{0,\ldots,0}^{i-1},G,\overbrace{0,\ldots,0}^{N-i})$*, and pairing* $e : \mathbb{V}\times\mathbb{V}\to\mathbb{G}_T$*. The pairing is defined by* $e(\boldsymbol{x},\boldsymbol{y}) := \prod_{i=1}^N e(G_i,H_i) \in \mathbb{G}_T$ *where* $\boldsymbol{x} := (G_1,\ldots,G_N) \in \mathbb{V}$ *and* $\boldsymbol{y} := (H_1,\ldots,H_N) \in \mathbb{V}$*. This is nondegenerate bilinear i.e.,* $e(s\boldsymbol{x},t\boldsymbol{y}) = e(\boldsymbol{x},\boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x},\boldsymbol{y}) = 1$ *for all* $\boldsymbol{y}\in\mathbb{V}$*, then* $\boldsymbol{x}=\boldsymbol{0}$*. For all* i *and* j*,* $e(\boldsymbol{a}_i,\boldsymbol{a}_j) = e(G,G)^{\delta_{i,j}}$ *where* $\delta_{i,j}=1$ *if* $i=j$*, and* 0 *otherwise, and* $e(G,G)\neq 1\in\mathbb{G}_T$*.*

DPVS also has linear transformations $\phi_{i,j}$ *on* $\mathbb{V}$ *s.t.* $\phi_{i,j}(\boldsymbol{a}_j)=\boldsymbol{a}_i$ *and* $\phi_{i,j}(\boldsymbol{a}_k)=\boldsymbol{0}$ *if* $k\neq j$*, which can be easily achieved by* $\phi_{i,j}(\boldsymbol{x}) := (\overbrace{0,\ldots,0}^{i-1},G_j,\overbrace{0,\ldots,0}^{N-i})$ *where* $\boldsymbol{x} := (G_1,\ldots,G_N)$*. We call* $\phi_{i,j}$ *"canonical maps". DPVS generation algorithm* $\mathcal{G}_{\mathsf{dpvs}}$ *takes input* 1^λ *(*$\lambda\in\mathbb{N}$*) and* $N\in\mathbb{N}$*, and outputs a description of* $\mathsf{param}'_{\mathbb{V}} := (q,\mathbb{V},\mathbb{G}_T,\mathbb{A},e)$ *with security parameter* λ *and* N*-dimensional* $\mathbb{V}$*. It can be constructed by using* $\mathcal{G}_{\mathsf{bpg}}$*.*

Definition 3 (DLIN: Decisional Linear Assumption [6]) *The DLIN problem is to guess* $\beta\in\{0,1\}$*, given* $(\mathsf{param}_{\mathbb{G}},\ G,\xi G,\kappa G,\delta\xi G,\sigma\kappa G,Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$*, where* $\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda) : \mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,G,e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \kappa,\delta,\xi,\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q, Y_0 := (\delta+\sigma)G, Y_1 \xleftarrow{\mathsf{U}} \mathbb{G}, \text{return } (\mathsf{param}_{\mathbb{G}},G,\xi G,\kappa G,\delta\xi G,\sigma\kappa G,Y_\beta)$*, for* $\beta\xleftarrow{\mathsf{U}}\{0,1\}$*. For a probabilistic machine* $\mathcal{E}$*, we define the advantage of* $\mathcal{E}$ *for the DLIN problem as:* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{E}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho\xleftarrow{\mathsf{R}}\mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda,\varrho)\to 1 \,\middle|\, \varrho\xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right]\right|$*. The DLIN assumption is: For any probabilistic polynomial-time adversary* $\mathcal{E}$*, the advantage* $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ *is negligible in* λ*.*

3 Definitions of (Hierarchical) Inner Product Encryption

3.1 Definition of Inner-Product Encryption (IPE)

This section defines predicate encryption (PE) for the class of inner-product predicates, i.e., inner product encryption (IPE) and its security.

An attribute of inner-product predicates is expressed as a vector $\vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$ and a predicate $f_{\vec{v}}$ is associated with a vector $\vec{v}$, where $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{v} \cdot \vec{x} = 0$. Let $\Sigma := \mathbb{F}_q^n \setminus \{\vec{0}\}$, i.e., the set of the attributes, and $\mathcal{F} := \{f_{\vec{v}} | \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\}\}$ i.e., the set of the predicates.

Definition 4 *An inner product encryption scheme (for predicates $\mathcal{F}$ and attributes Σ) consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}$ *and* Dec. *They are given as follows:*

- Setup *takes as input security parameter 1^λ outputs (master) public key* pk *and (master) secret key* sk.
- KeyGen *takes as input the master public key* pk, *secret key* sk, *and predicate vector $\vec{v}$. It outputs a corresponding secret key $\mathsf{sk}_{\vec{v}}$.*
- Enc *takes as input the master public key* pk, *plaintext m in some associated plaintext space,* msg, *and attribute vector $\vec{x}$. It returns ciphertext $\mathsf{ct}_{\vec{x}}$.*
- Dec *takes as input the master public key* pk, *secret key $\mathsf{sk}_{\vec{v}}$ and ciphertext $\mathsf{ct}_{\vec{x}}$. It outputs either plaintext m or the distinguished symbol $\perp$.*

An IPE scheme should have the following correctness property: for all $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$, all $f_{\vec{v}} \in \mathcal{F}$ and $\vec{x} \in \Sigma$, all $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$, all messages m, all ciphertext $\mathsf{ct}_{\vec{x}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m, \vec{x})$, it holds that $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{\vec{v}}, \mathsf{ct}_{\vec{x}})$ if $f_{\vec{v}}(\vec{x}) = 1$. Otherwise, it holds with negligible probability.

We then define the security notion of IPE, that was called "*adaptively* secure and *fully attribute-hiding*" in Abstract and Section 1. Since we will deal with only this security notion hereafter, we shortly call it "*adaptively attribute-hiding*."

Definition 5 *The model for defining the adaptively attribute-hiding security of IPE against adversary $\mathcal{A}$ (under chosen plaintext attacks) is given as follows:*

1. Setup *is run to generate keys* pk *and* sk, *and* pk *is given to $\mathcal{A}$.*
2. *$\mathcal{A}$ may adaptively make a polynomial number of key queries for predicate vectors, $\vec{v}$. In response, $\mathcal{A}$ is given the corresponding key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$.*
3. *$\mathcal{A}$ outputs challenge attribute vector $(\vec{x}^{(0)}, \vec{x}^{(1)})$ and challenge plaintexts $(m^{(0)}, m^{(1)})$, subject to the following restrictions:*
   - *$\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$ for all the key queried predicate vectors, $\vec{v}$.*
   - *Two challenge plaintexts are equal, i.e., $m^{(0)} = m^{(1)}$, and any key query $\vec{v}$ satisfies $f_{\vec{v}}(\vec{x}^{(0)}) = f_{\vec{v}}(\vec{x}^{(1)})$, i.e., one of the following conditions.*
     - *$\vec{v} \cdot \vec{x}^{(0)} = 0$ and $\vec{v} \cdot \vec{x}^{(1)} = 0$,*
     - *$\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$,*
4. *A random bit b is chosen. $\mathcal{A}$ is given $\mathsf{ct}_{\vec{x}^{(b)}} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \vec{x}^{(b)})$.*
5. *The adversary may continue to issue key queries for additional predicate vectors, $\vec{v}$, subject to the restriction given in step 3. $\mathcal{A}$ is given the corresponding key $\mathsf{sk}_{\vec{v}} \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v})$.*
6. *$\mathcal{A}$ outputs a bit b', and wins if $b' = b$.*

The advantage of $\mathcal{A}$ in the above game is defined as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH}}(\lambda) := \mathsf{Pr}[\mathcal{A} \text{ wins }] - 1/2$ *for any security parameter λ. An IPE scheme is* adaptively attribute-hiding (AH) against chosen plaintext attacks *if all probabilistic polynomial-time adversaries $\mathcal{A}$ have at most negligible advantage in the above game.*

For each run of the game, the variable s is defined as $s := 0$ if $m^{(0)} \neq m^{(1)}$ for challenge plaintexts $m^{(0)}$ and $m^{(1)}$, and $s := 1$ otherwise.

3.2 Definition of Hierarchical Inner-Product Encryption (HIPE)

This section defines hierarchical inner product encryption (HIPE) and its security.

In a delegation system, it is required that a user who has a capability can delegate to another user a more restrictive capability. In addition to this requirement, our hierarchical inner-product encryption introduces a format of hierarchy $\vec{n}$ to define common delegation structure in a system.

We call a tuple of positive integers $\vec{n} := (d; n_1, \ldots, n_d)$ a format of hierarchy of depth d attribute spaces. Let Σ_ℓ $(\ell = 1, \ldots, d)$ be the sets of attributes, where each $\Sigma_\ell := \mathbb{F}_q^{n_\ell} \setminus \{\vec{0}\}$. Let the hierarchical attributes $\Sigma := \cup_{\ell=1}^{d}(\Sigma_1 \times \ldots \times \Sigma_\ell)$, where the union is a disjoint union. Then, for $\vec{v}_i \in \mathbb{F}_q^{n_i} \setminus \{\vec{0}\}$, the hierarchical predicate $f_{(\vec{v}_1,\ldots,\vec{v}_\ell)}$ on hierarchical attributes $(\vec{x}_1, \ldots, \vec{x}_h) \in \Sigma$ is defined as follows: $f_{(\vec{v}_1,\ldots,\vec{v}_\ell)}(\vec{x}_1, \ldots, \vec{x}_h) = 1$ iff $\ell \leq h$ and $\vec{x}_i \cdot \vec{v}_i = 0$ for all i s.t. $1 \leq i \leq \ell$.

Let the space of hierarchical predicates $\mathcal{F} := \{f_{(\vec{v}_1,\ldots,\vec{v}_\ell)} \mid \vec{v}_i \in \mathbb{F}_q^{n_i} \setminus \{\vec{0}\}\}$. We call h (resp. ℓ) the level of $(\vec{x}_1, \ldots, \vec{x}_h)$ (resp. $(\vec{v}_1, \ldots, \vec{v}_\ell)$).

Definition 6 *Let $\vec{n} := (d; n_1, \ldots, n_d)$ be a format of hierarchy of depth d attribute spaces. A hierarchical inner product encryption (HIPE) scheme for the class of hierarchical predicates $\mathcal{F}$ over the set of hierarchical attributes Σ consists of probabilistic polynomial-time algorithms* $\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}$, *and* $\mathsf{Delegate}_\ell$ *for $\ell = 1, \ldots, d-1$. They are given as follows:*

- Setup *takes as input security parameter 1^λ and format of hierarchy $\vec{n}$, and outputs (master) public key* pk *and (master) secret key* sk.
- KeyGen *takes as input the master public key* pk, *secret key* sk, *and predicate vectors $(\vec{v}_1, \ldots, \vec{v}_\ell)$. It outputs a corresponding secret key* $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_\ell)}$.
- Enc *takes as input the master public key* pk, *attribute vectors $(\vec{x}_1, \ldots, \vec{x}_h)$, where $1 \leq h \leq d$, and plaintext m in some associated plaintext space,* msg. *It returns ciphertext c.*
- Dec *takes as input the master public key* pk, *secret key* $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_\ell)}$, *where $1 \leq \ell \leq d$, and ciphertext c. It outputs either plaintext m or the distinguished symbol $\perp$.*
- $\mathsf{Delegate}_\ell$ *takes as input the master public key* pk, *ℓ-th level secret key* $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_\ell)}$, *and $(\ell+1)$-th level predicate vector $\vec{v}_{\ell+1}$. It returns $(\ell+1)$-th level secret key* $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_{\ell+1})}$.

A HIPE scheme should have the following correctness property: for all correctly generated pk and $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_\ell)}$, generate $c \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m, (\vec{x}_1, \ldots, \vec{x}_h))$ and $m' := \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_\ell)}, c)$. If $f_{(\vec{v}_1,\ldots,\vec{v}_\ell)}(\vec{x}_1, \ldots, \vec{x}_h) = 1$, then $m' = m$. Otherwise, $m' \neq m$ except for negligible probability.

For f and f' in $\mathcal{F}$, we denote $f' \leq f$ if the predicate vector for f is a prefix of that for f'. For the following definition for key queries, see [28].

Definition 7 *The model for defining the adaptively attribute-hiding security of HIPE against adversary $\mathcal{A}$ (under chosen plaintext attacks) is given as follows:*

1. Setup *is run to generate keys* pk *and* sk, *and* pk *is given to $\mathcal{A}$.*

2. *$\mathcal{A}$ may adaptively makes a polynomial number of queries of the following type:*

   - *[Create key] $\mathcal{A}$ asks the challenger to create a secret key for a predicate $f \in \mathcal{F}$. The challenger creates a key for f without giving it to $\mathcal{A}$.*
   - *[Create delegated key] $\mathcal{A}$ specifies a key for predicate f that has already been created, and asks the challenger to perform a delegation operation to create a child key for $f' \leq f$. The challenger computes the child key without giving it to the adversary.*
   - *[Reveal key] $\mathcal{A}$ asks the challenger to reveal an already-created key for predicate f.*

   Note that when key creation requests are made, $\mathcal{A}$ does not automatically see the created key. $\mathcal{A}$ sees a key only when it makes a reveal key query.

3. *$\mathcal{A}$ outputs challenge attribute vectors $\mathcal{X}^{(0)} := (\vec{x}_1^{(0)}, \ldots, \vec{x}_{h^{(0)}}^{(0)}), \mathcal{X}^{(1)} := (\vec{x}_1^{(1)}, \ldots, \vec{x}_{h^{(1)}}^{(1)})$ and challenge plaintexts $m^{(0)}, m^{(1)}$, subject to the following restrictions:*

   - *$f(\mathcal{X}^{(0)}) = f(\mathcal{X}^{(1)}) = 0$ for all the reveal key queried predicate f.*
   - *Two challenge plaintexts are equal, i.e., $m^{(0)} = m^{(1)}$ and reveal key queried predicate f satisfies $f(\mathcal{X}^{(0)}) = f(\mathcal{X}^{(1)})$, i.e., one of the following conditions.*
     - *$f(\mathcal{X}^{(0)}) = f(\mathcal{X}^{(1)}) = 1$,*
     - *$f(\mathcal{X}^{(0)}) = f(\mathcal{X}^{(1)}) = 0$.*

4. *A random bit b is chosen. $\mathcal{A}$ is given $c^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, m^{(b)}, \mathcal{X}^{(b)})$.*

5. *The adversary may continue to request keys for additional predicate vectors subject to the restriction given in step 3. $\mathcal{A}$ is given a reply as in step 2.*

6. *$\mathcal{A}$ outputs a bit b', and succeeds if $b' = b$.*

The advantage of $\mathcal{A}$ in the above game is defined as $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{HIPE,AH}}(\lambda) := \mathsf{Pr}[b' = b] - 1/2$ for any security parameter λ. A HIPE scheme is adaptively attribute-hiding (AH) against chosen plaintext attacks *if all probabilistic polynomial-time adversaries $\mathcal{A}$ have at most negligible advantage in the above game.*

For each run of the game, the variable s is defined as $s := 0$ if $m^{(0)} \neq m^{(1)}$ for challenge plaintexts $m^{(0)}$ and $m^{(1)}$, and $s := 1$ otherwise.

Remark 1 In the definition, the levels $h^{(0)}$ and $h^{(1)}$ of the two challenge vectors given by an adversary, $(\vec{x}_i^{(0)})_{i=1,\ldots,h^{(0)}}$ and $(\vec{x}_i^{(1)})_{i=1,\ldots,h^{(1)}}$, can be different, i.e., $h^{(0)} \neq h^{(1)}$ is allowed. The proposed HIPE scheme only satisfies the security definition under the restriction that $h^{(0)} = h^{(1)}$. Here, this restricted security ensures the anonymity of attributes of a ciphertext but with revealing the number of levels of attributes, while the above security definition ensures the anonymity of attributes as well as the number of levels. (The HIPE scheme in [20] satisfies the unrestricted security.) Our HIPE scheme can be modified to satisfy the unrestricted security as: when generating a ciphertext in Enc, input vectors $(\vec{x}_i)_{i=1,\ldots,\ell}$ are padded with random vectors $(\vec{x}_i)_{i=\ell+1,\ldots,d}$ for a maximum level d, in the same manner as the HIPE in [20].

4 Proposed (Basic) IPE Scheme

4.1 Dual Orthonormal Basis Generator

We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}$ below, which is used as a subroutine in the proposed IPE scheme.

$\mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, N)$: $\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N), \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G,G)^\psi,$
$X := (\chi_{i,j}) \xleftarrow{\mathsf{U}} GL(N, \mathbb{F}_q),\ (\vartheta_{i,j}) := \psi \cdot (X^{\mathrm{T}})^{-1},\ \mathsf{param}_{\mathbb{V}} := (\mathsf{param}'_{\mathbb{V}}, g_T),$
$\boldsymbol{b}_i := \sum_{j=1}^N \chi_{i,j} \boldsymbol{a}_j, \mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N),\ \boldsymbol{b}_i^* := \sum_{j=1}^N \vartheta_{i,j} \boldsymbol{a}_j, \mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*),$
return $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*)$.

4.2 Construction

In the description of the scheme, we assume that the first coordinate, x_1, of input vector, $\vec{x} := (x_1, \ldots, x_n)$, is nonzero. Random dual basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, N)$ is defined at the end of Section 2. We refer to Section 1.4 for notations on DPVS.

$\mathsf{Setup}(1^\lambda,\ n)$:
$(\mathsf{param}_{\mathbb{V}}, \mathbb{B} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{4n+1}), \mathbb{B}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_{4n+1}^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, 4n+2),$
$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}),\ \ \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{b}_{3n+1}^*, \ldots, \boldsymbol{b}_{4n}^*),$
return $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}),\ \mathsf{sk} := \widehat{\mathbb{B}}^*$.

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, \vec{v} \in \mathbb{F}_q^n \setminus \{\vec{0}\})$: $\sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n,$

$$\boldsymbol{k}^* := (\ \overbrace{1}^{1},\ \overbrace{\sigma\vec{v}}^{n},\ \overbrace{0^{2n}}^{2n},\ \overbrace{\vec{\eta}}^{n},\ \overbrace{0}^{1}\ )_{\mathbb{B}^*},$$

return $\mathsf{sk}_{\vec{v}} := \boldsymbol{k}^*$.

$\mathsf{Enc}(\mathsf{pk},\ m, \vec{x} \in \mathbb{F}_q^n \setminus \{\vec{0}\})$: $\omega, \varphi, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$$\boldsymbol{c}_1 := (\ \overbrace{\zeta}^{1},\ \overbrace{\omega\vec{x}}^{n},\ \overbrace{0^{2n}}^{2n},\ \overbrace{0^n}^{n},\ \overbrace{\varphi}^{1}\ )_{\mathbb{B}}, \qquad c_2 := g_T^\zeta m,$$

return $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := \boldsymbol{k}^*,\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$: $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$, return m'.

[Correctness] If $\vec{v} \cdot \vec{x} = 0$, then $e(\boldsymbol{c}_1, \boldsymbol{k}^*) = g_T^{\zeta + \omega\sigma\vec{v}\cdot\vec{x}} = g_T^\zeta$.

4.3 Security

4.3.1 Main Theorem (Theorem 1) and Main Lemma (Lemma 1)

Theorem 1 *The proposed IPE scheme is adaptively attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{0\text{-}1}, \mathcal{E}_{0\text{-}2}, \mathcal{E}_{1\text{-}1}, \mathcal{E}_{1\text{-}2\text{-}1}$ and $\mathcal{E}_{1\text{-}2\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IPE,AH}}(\lambda) \le \mathsf{Adv}_{\mathcal{E}_{0\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \sum_{h=1}^{\nu} \left(\mathsf{Adv}_{\mathcal{E}_{0\text{-}2\text{-}h}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}}^{\mathsf{DLIN}}(\lambda) + \mathsf{Adv}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}}^{\mathsf{DLIN}}(\lambda) \right) + \epsilon,$$

where $\mathcal{E}_{0\text{-}2\text{-}h}(\cdot) := \mathcal{E}_{0\text{-}2}(h, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}1}(h, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}2}(h, \cdot)$, ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (29\nu + 17)/q$.

Proof. First, we execute a preliminary game transformation from Game 0 (original security game in Definition 5) to Game 0', which is the same as Game 0 except that flip a coin $t \xleftarrow{\mathsf{U}} \{0,1\}$ before setup, and the game is aborted in step 3 if $t \neq s$. We define that $\mathcal{A}$ wins with probability $1/2$ when the game is aborted (and the advantage in Game 0' is $\mathsf{Pr}[\mathcal{A} \text{ wins }] - 1/2$ as well). Since t is independent from s, the game is aborted with probability $1/2$. Hence, the advantage in Game 0' is a half of that in Game 0, i.e., $\mathsf{Adv}^{\mathsf{IPE,AH},0'}_{\mathcal{A}}(\lambda) = 1/2 \cdot \mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda)$. Moreover, $\Pr[\mathcal{A} \text{ wins}] = 1/2 \cdot (\Pr[\mathcal{A} \text{ wins} \mid t=0] + \Pr[\mathcal{A} \text{ wins} \mid t=1])$ in Game 0' since t is uniformly and independently generated.

As for the conditional probability with $t = 0$, it holds that, for any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1$ and $\mathcal{E}_2$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, in Game 0',

$$\Pr[\mathcal{A} \text{ wins} \mid t=0] - 1/2 \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \textstyle\sum_{h=1}^{\nu} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h}}(\lambda) + \epsilon,$$

where $\mathcal{E}_{2\text{-}h}(\cdot) := \mathcal{E}_2(h,\cdot)$ and ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (6\nu+5)/q$. This is obtained in the same manner as the weakly attribute-hiding security of the OT10 IPE in the full version of [23]: Since the difference between our IPE and the OT10 IPE is only the dimension of the hidden subspaces, i.e., the former has $2n$ and the latter has n, the weakly attribute-hiding security of the OT10 IPE implies the security with $t = 0$ of our IPE.

As for the conditional probability with $t = 1$, i.e., $\Pr[\mathcal{A} \text{ wins} \mid t=1]$, Lemma 1 (Eq. (1)) holds. Therefore,

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) &= 2 \cdot \mathsf{Adv}^{\mathsf{IPE,AH},0'}_{\mathcal{A}}(\lambda) = \Pr[\mathcal{A} \text{ wins} \mid t=0] + \Pr[\mathcal{A} \text{ wins} \mid t=1] - 1 \\
&= (\Pr[\mathcal{A} \text{ wins} \mid t=0] - 1/2) + (\Pr[\mathcal{A} \text{ wins} \mid t=1] - 1/2) \\
&\leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}1}}(\lambda) + \textstyle\sum_{h=1}^{\nu} \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}2\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) \\
&\quad + \textstyle\sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}}(\lambda)\right) + \epsilon, \text{ where } \epsilon := (29\nu+17)/q. \quad \square
\end{aligned}$$

Lemma 1 (Main Lemma) *For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_1, \mathcal{E}_{2\text{-}1}$ and $\mathcal{E}_{2\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, in Game 0' (described in the proof of Theorem 1),*

$$\begin{aligned}
&\Pr[\mathcal{A} \text{ wins} \mid t=1] - 1/2 \\
&\qquad \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu} \left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}2}}(\lambda)\right) + \epsilon, \qquad (1)
\end{aligned}$$

where $\mathcal{E}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{2\text{-}1}(h,\cdot)$, $\mathcal{E}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{2\text{-}2}(h,\cdot)$, ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (23\nu+12)/q$.

4.3.2 Proof Outline of Lemma 1

At the top level strategy of the security proof, an extended form of the dual system encryption by Waters [29] is employed, where ciphertexts and secret keys have three forms, *normal*, *temporal 1* and *temporal 2*. The real system uses only normal ciphertexts and normal secret keys, and temporal 1 and 2 ciphertexts and keys are used only in a sequence of security games for the security proof. (Additionally, ciphertexts have temporal 0 and unbiased forms. See below.)

To prove this lemma, we only consider the $t = 1$ case. We employ Game 0' (described in the proof of Theorem 1) through Game 3. In Game 1, the challenge ciphertext is changed to temporal 0 form. When at most ν secret key queries are issued by an adversary, there are 4ν game changes from Game 1 (Game 2-0-4), Game 2-1-1, Game 2-1-2, Game 2-1-3, Game 2-1-4 through Game 2-ν-1, Game 2-ν-2, Game 2-ν-3, Game 2-ν-4.

Table 1: Outline of Game Descriptions

Game	Challenge ciphertext	Queried keys				
		1	$\cdots$ $h-1$	h	$h+1$ $\cdots$	ν
0'	normal	normal				
1	temporal 0	normal				
2-1-1	temporal 1	normal				
2-1-2	temporal 1	temporal 1	normal			
2-1-3	temporal 2	temporal 1	normal			
2-1-4	temporal 2	temporal 2	normal			
$\vdots$						
2-h-1	temporal 1	temporal 2		normal		
2-h-2	temporal 1	temporal 2		temporal 1	normal	
2-h-3	temporal 2	temporal 2		temporal 1	normal	
2-h-4	temporal 2	temporal 2		temporal 2	normal	
$\vdots$						
2-ν-4	temporal 2	temporal 2				temporal 2
3	unbiased	temporal 2				

In Game 2-h-1, the challenge ciphertext is changed to temporal 1 form, and the first $h-1$ keys are temporal 2 form, while the remaining keys are normal. In Game 2-h-2, the h-th key is changed to temporal 1 form while the remaining keys and the challenge ciphertext is the same as in Game 2-h-1. In Game 2-h-3, the challenge ciphertext is changed to temporal 2 form while all the queried keys are the same as in Game 2-h-2. In Game 2-h-4, the h-th key is changed to temporal 2 form while the remaining keys and the challenge ciphertext is the same as in Game 2-h-3. At the end of the Game 2 sequence, in Game 2-ν-4, all the queried keys are temporal 2 forms (and the challenge ciphertext is temporal 2 form), which allows the next conceptual change to Game 3. In Game 3, the challenge ciphertext is changed to *unbiased* form (while all the queried keys are temporal 2 form). In the final game, advantage of the adversary is zero.

We summarize these changes in Table 1, where shaded parts indicate the challenge ciphertext or queried key(s) which were changed in a game from the previous game

As usual, we prove that the advantage gaps between neighboring games are negligible.

For $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$, we focus on $\boldsymbol{c}_1$, and ignore the other part of $\mathsf{ct}_{\vec{x}}$, i.e., c_2, (and call $\boldsymbol{c}_1$ ciphertext) in this proof outline. In addition, we ignore a negligible factor in the (informal) descriptions of this proof outline. For example, we say "A is bounded by B" when $A \leq B + \epsilon(\lambda)$ where $\epsilon(\lambda)$ is negligible in security parameter λ.

A normal secret key, $\boldsymbol{k}^{*\,\mathsf{norm}}$ (with vector $\vec{v}$), is the correct form of the secret key of the proposed IPE scheme, and is expressed by Eq. (2). Similarly, a normal ciphertext (with vector $\vec{x}$), $\boldsymbol{c}_1^{\mathsf{norm}}$, is expressed by Eq. (3). A temporal 0 ciphertext is expressed by Eq. (4). A temporal 1 ciphertext, $\boldsymbol{c}_1^{\mathsf{temp1}}$, is expressed by Eq. (5) and a temporal 1 secret key, $\boldsymbol{k}^{*\,\mathsf{temp1}}$, is expressed by Eq. (6). A temporal 2 ciphertext, $\boldsymbol{c}_1^{\mathsf{temp2}}$, is expressed by Eq. (7) and a temporal 2 secret key, $\boldsymbol{k}^{*\,\mathsf{temp2}}$, is expressed by Eq. (8). An unbiased ciphertext, $\boldsymbol{c}_1^{\mathsf{unbias}}$, is expressed by Eq. (9).

To prove that the advantage gap between Games 0' and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0,1\}$), we construct a simulator of the challenger of Game 0' (or 1)

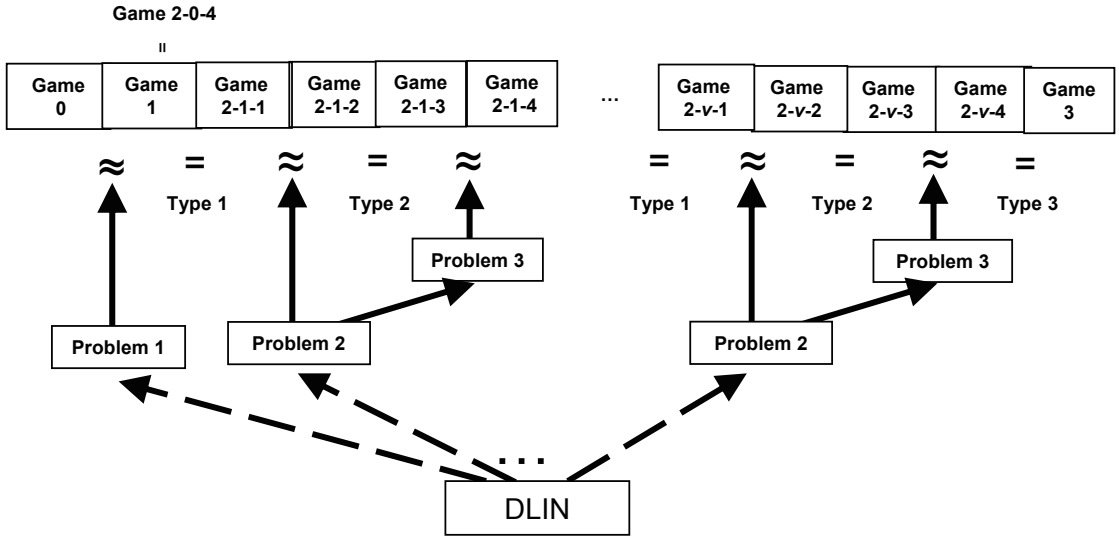

Figure 1: Structure of Reductions

(against an adversary $\mathcal{A}$) by using an instance with $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ of Problem 1. We then show that the distribution of the secret keys and challenge ciphertext replied by the simulator is equivalent to those of Game 0' when $\beta = 0$ and those of Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0' and 1 (Lemma 6). The advantage of Problem 1 is proven to be equivalent to that of the DLIN assumption (Lemma 2).

We then show that Game 2-$(h-1)$-4 can be conceptually changed to Game 2-h-1 (Lemma 7), by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{2n})$ and $(\boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary. In particular, when $h = 1$, it means that Game 1 can be conceptually changed to Game 2-1-1. When $h \geq 2$, we notice that temporal 2 key and temporal 1 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp2}}, \boldsymbol{c}_1^{\mathsf{temp1}})$, are equivalent to temporal 2 key and temporal 2 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp2}}, \boldsymbol{c}_1^{\mathsf{temp2}})$, except that $\vec{x}^{(b)}$ is used in $\boldsymbol{c}_1^{\mathsf{temp1}}$ instead of $\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)}$ (with $\omega'_0, \omega'_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$) for some coefficient vector in $\boldsymbol{c}_1^{\mathsf{temp2}}$. This change of coefficient vectors can be done conceptually since zero vector 0^n is used for the corresponding part in $\boldsymbol{k}^{*\,\mathsf{temp2}}$.

The advantage gap between Games 2-h-1 and 2-h-2 is shown to be bounded by the advantage of Problem 2, i.e., advantage of the DLIN assumption (Lemmas 8 and 3).

We then show that Game 2-h-2 can be conceptually changed to Game 2-h-3 (Lemma 9), again by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{2n})$ and $(\boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary. In this conceptual change, we use the fact that all key queries $\vec{v}$ satisfy $\vec{v} \cdot \vec{x}^{(0)} = \vec{v} \cdot \vec{x}^{(1)} = 0$ or $\vec{v} \cdot \vec{x}^{(0)} \neq 0$ and $\vec{v} \cdot \vec{x}^{(1)} \neq 0$. Here, we notice that temporal 1 key and temporal 1 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp1}}, \boldsymbol{c}_1^{\mathsf{temp1}})$, are equivalent to temporal 1 key and temporal 2 challenge ciphertext, $(\boldsymbol{k}^{*\,\mathsf{temp1}}, \boldsymbol{c}_1^{\mathsf{temp2}})$, except that random linear combination $\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)}$ (with $\omega'_0, \omega'_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$) is used in $\boldsymbol{c}_1^{\mathsf{temp2}}$ instead of $\vec{x}^{(b)}$ for some coefficient vector in $\boldsymbol{c}_1^{\mathsf{temp1}}$. This conceptual change is proved by using Lemma 5.

The advantage gap between Games 2-h-3 and 2-h-4 is similarly shown to be bounded by the advantage of Problem 3, i.e., advantage of the DLIN assumption (Lemmas 10 and 4).

We then show that Game 2-ν-4 can be conceptually changed to Game 3 (Lemma 11) by using the fact that parts of bases, $(\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{3n})$ and $(\boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_{2n})$, are unknown to the adversary.

Figure 1 shows the structure of the security reduction, where the security of the scheme is

hierarchically reduced to the intractability of the DLIN problem. The reduction steps indicated by dotted arrows can be shown in the same manner as that in (the full version of) [23].

4.3.3 Proof of Lemma 1

To prove Lemma 1, we consider the following $4\nu + 3$ games when $t = 1$. In Game 0', a part framed by a box indicates coefficients to be changed in a subsequent game. In the other games, a part framed by a box indicates coefficients which were changed in a game from the previous game.

Game 0' : Same as Game 0 except that flip a coin $t \xleftarrow{\cup} \{0,1\}$ before setup, and the game is aborted in step 3 if $t \neq s$. In order to prove Lemma 1, we consider the case with $t = 1$. The reply to a key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{0^n},\ \boxed{0^n},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \tag{2}$$

where $\sigma \xleftarrow{\cup} \mathbb{F}_q$ and $\vec{\eta} \xleftarrow{\cup} \mathbb{F}_q^n$. The challenge ciphertext for challenge plaintext $m := m^{(0)} = m^{(1)}$ and vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \boxed{\omega\vec{x}^{(b)}},\ \boxed{0^n},\ \boxed{0^n},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \quad c_2 := g_T^{\zeta} m, \tag{3}$$

where $b \xleftarrow{\cup} \{0,1\}$ and $\zeta, \omega, \varphi \xleftarrow{\cup} \mathbb{F}_q$. Here, we note that c_2 is independent from bit b.

Game 1 : Game 1 is the same as Game 0' except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintext $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{zx_1^{(b)}, 0^{n-1}},\ 0^n,\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{4}$$

where $x_1^{(b)} \neq 0$ is the first coordinate of $\vec{x}^{(b)}$, $z \xleftarrow{\cup} \mathbb{F}_q$ and all the other variables are generated as in Game 0'.

Game 2-h-1 ($h = 1, \ldots, \nu$) : Game 2-0-4 is Game 1. Game 2-h-1 is the same as Game 2-$(h-1)$-4 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintext $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\omega'\vec{x}^{(b)}},\ \boxed{\omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)}},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{5}$$

where $\omega', \omega_0'', \omega_1'' \xleftarrow{\cup} \mathbb{F}_q$ and all the other variables are generated as in Game 2-$(h-1)$-4.

Game 2-h-2 ($h = 1, \ldots, \nu$) : Game 2-h-2 is the same as Game 2-h-1 except that the reply to the h-th key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{\sigma'\vec{v}},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \tag{6}$$

where $\sigma' \xleftarrow{\cup} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-1.

Game 2-h-3 ($h = 1, \ldots, \nu$) : Game 2-h-3 is the same as Game 2-h-2 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)}},\ \omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{7}$$

where $\omega_0', \omega_1' \xleftarrow{\cup} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-2.

Game 2-h-4 ($h = 1, \ldots, \nu$) : Game 2-h-4 is the same as Game 2-h-3 except that the reply to the h-th key query for $\vec{v}$ is:

$$\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{0^n},\ \boxed{\sigma''\vec{v}},\ \vec{\eta},\ 0\ )_{\mathbb{B}^*}, \tag{8}$$

where $\sigma'' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-h-3.

Game 3 : Game 3 is the same as Game 2-ν-4 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \boxed{\omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)}},\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{9}$$

where $\omega_0, \omega_1 \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and all the other variables are generated as in Game 2-ν-4. Here, we note that $\boldsymbol{c}_1$ is independent from bit $b \xleftarrow{\mathsf{U}} \{0,1\}$.

Let $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda), \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda), \ldots, \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)$ be the advantage of $\mathcal{A}$ in Game $0', 1, 2\text{-}h\text{-}1, \ldots, 2\text{-}h\text{-}4$ and 3 when $t = 1$, respectively. $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda)$ is equivalent to the left-hand side of Eq. (1). We will show six lemmas (Lemmas 6–11) that evaluate the gaps between pairs of neighboring games. From these lemmas and Lemmas 2–4, we obtain $\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) \leq \left|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)\right| + \sum_{h=1}^{\nu}\left(\left|\mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda)\right| + \sum_{\iota=2}^{4}\left|\mathsf{Adv}^{(2\text{-}h\text{-}(\iota-1))}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}\iota)}_{\mathcal{A}}(\lambda)\right|\right) + \left|\mathsf{Adv}^{(2\text{-}\nu\text{-}4)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda)\right| + \mathsf{Adv}^{(3)}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda) + \sum_{h=1}^{\nu}\left(\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{2\text{-}h\text{-}2}}(\lambda)\right) + (4\nu+1)/q \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_1}(\lambda) + \sum_{h=1}^{\nu}\left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{2\text{-}h\text{-}2}}(\lambda)\right) + (23\nu+12)/q.$ □

4.3.4 Lemmas 2–12

Definition 8 (Problem 1) *Problem 1 is to guess β, given $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_{\beta}(1^\lambda, n)$, where*

$$\begin{aligned}
&\mathcal{G}^{\mathsf{P1}}_{\beta}(1^\lambda, n):\ (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 4n+2),\\
&\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n+1}), \quad \omega, \gamma, z \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\qquad \overbrace{}^{1}\ \overbrace{\phantom{\omega\vec{e}_1}}^{n}\ \overbrace{\phantom{0^{2n}}}^{2n}\ \overbrace{}^{n}\ \overbrace{}^{1}\\
&\boldsymbol{e}_{0,1} := (\ 0,\ \omega\vec{e}_1,\ 0^{2n},\ 0^n,\ \gamma\ )_{\mathbb{B}},\\
&\boldsymbol{e}_{1,1} := (\ 0,\ \omega\vec{e}_1,\ z\vec{e}_1,\ 0^n,\ 0^n,\ \gamma\ )_{\mathbb{B}},\\
&\boldsymbol{e}_i := \omega\boldsymbol{b}_i \ \text{ for } i = 2, \ldots, n,\\
&\text{return } (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n}),
\end{aligned}$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 1 as: $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) := \left|\mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_1(1^\lambda, n)\right]\right|$.

Lemma 2 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 6/q$.*

Proof. Problem 1 is essentially same as Basic Problem 1 in [23], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 2 is proven in a similar manner as the reduction lemmas in [23]. □

Definition 9 (Problem 2) *Problem 2 is to guess β, given* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_{\beta}(1^\lambda, n)$, *where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P2}}_{\beta}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 4n+2),\\
&\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{4n+1}), \quad \delta, \tau, \delta_0, \omega, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad \text{for } i = 1, \ldots, n;\\
&\qquad\qquad \overbrace{}^{1} \quad \overbrace{\phantom{\delta\vec{e}_i,}}^{n} \quad \overbrace{}^{n} \quad \overbrace{}^{n} \quad \overbrace{\phantom{\delta_0\vec{e}_i,}}^{n} \quad \overbrace{}^{1}\\
&\quad \boldsymbol{h}^*_{0,i} := (\ 0, \quad \delta\vec{e}_i, \quad 0^n, \quad 0^n, \quad \delta_0\vec{e}_i, \quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{h}^*_{1,i} := (\ 0, \quad \delta\vec{e}_i, \quad \tau\vec{e}_i, \quad 0^n, \quad \delta_0\vec{e}_i, \quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{e}_i := (\ 0, \quad \omega\vec{e}_i, \quad \sigma\vec{e}_i, \quad 0^n, \quad 0^n, \quad 0\ )_{\mathbb{B}},\\
&\quad \text{return } (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 2, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 3 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 5/q$.*

Proof. Problem 2 is essentially same as Basic Problem 2 in [23], where the intractability of the problem is reduced to that of DLIN. Therefore, Lemma 3 is proven in a similar manner as the reduction lemmas in [23]. □

Definition 10 (Problem 3) *Problem 3 is to guess β, given* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P3}}_{\beta}(1^\lambda, n)$, *where*

$$
\begin{aligned}
&\mathcal{G}^{\mathsf{P3}}_{\beta}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{IPE}}_{\mathsf{ob}}(1^\lambda, 4n+2),\\
&\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{b}^*_{4n+1}),\\
&\quad \tau, \delta_0, \omega', \omega'', \kappa', \kappa'' \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\quad \text{for } i = 1, \ldots, n;\\
&\qquad\qquad \overbrace{\phantom{0^{n+1},}}^{n+1} \quad \overbrace{\phantom{\tau\vec{e}_i,}}^{n} \quad \overbrace{}^{n} \quad \overbrace{\phantom{\delta_0\vec{e}_i,}}^{n} \quad \overbrace{}^{1}\\
&\quad \boldsymbol{h}^*_{0,i} := (\ 0^{n+1}, \quad \tau\vec{e}_i, \quad 0^n, \quad \delta_0\vec{e}_i, \quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{h}^*_{1,i} := (\ 0^{n+1}, \quad 0^n, \quad \tau\vec{e}_i, \quad \delta_0\vec{e}_i, \quad 0\ )_{\mathbb{B}^*}\\
&\quad \boldsymbol{e}_i := (\ 0^{n+1}, \quad \omega'\vec{e}_i, \quad \omega''\vec{e}_i, \quad 0^n, \quad 0\ )_{\mathbb{B}},\\
&\quad \boldsymbol{f}_i := (\ 0^{n+1}, \quad \kappa'\vec{e}_i, \quad \kappa''\vec{e}_i, \quad 0^n, \quad 0\ )_{\mathbb{B}},\\
&\quad \text{return } (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n}),
\end{aligned}
$$

for $\beta \xleftarrow{\mathsf{U}} \{0,1\}$. For a probabilistic adversary $\mathcal{B}$, the advantage of $\mathcal{B}$ for Problem 3, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda)$, is similarly defined as in Definition 8.

Lemma 4 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{E}$, whose running time is essentially the same as that of $\mathcal{B}$, such that for any security parameter λ, $\mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}}(\lambda) + 8/q$.*

Lemma 5 (Lemma 3 in [23]) *For $p \in \mathbb{F}_q$, let $C_p := \{(\vec{x}, \vec{v}) | \vec{x} \cdot \vec{v} = p\} \subset V \times V^*$ where V is n-dimensional vector space $\mathbb{F}_q^n$, and V^* its dual. For all $(\vec{x}, \vec{v}) \in C_p$, for all $(\vec{r}, \vec{w}) \in C_p$, $\Pr[\vec{x}U = \vec{r} \wedge \vec{v}Z = \vec{w}] = \Pr[\vec{x}Z = \vec{r} \wedge \vec{v}U = \vec{w}] = 1/\sharp C_p$, where $Z \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q), U := (Z^{-1})^{\mathrm{T}}$.*

Lemma 6 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda)$.*

Lemma 7 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq 2/q$.*

Lemma 8 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}1}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P2}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{2\text{-}1}(h, \cdot)$.*

Lemma 9 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda)| \leq 8/q$.*

Lemma 10 *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_{2\text{-}2}$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}4)}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2}}^{\mathsf{P3}}(\lambda)$, where $\mathcal{B}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \cdot)$.*

Lemma 11 *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$.*

Lemma 12 *For any adversary $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$.*

Proof. The value of b is independent from $\mathcal{A}$'s view in Game 3. Hence, $\mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda) = 0$. □

The proofs of Lemmas 4, 6–11 are given in Appendix B.

5 A Variant for Achieving Shorter Public and Secret Keys

A variant of the proposed (basic) IPE scheme with the same security, that achieves a shorter ($O(n)$-size) master public key and shorter ($O(1)$-size) secret keys (excluding the description of $\vec{v}$), can be constructed by combining with the techniques in [24], where n is the dimension of vectors of the IPE scheme. This variant also enjoys more efficient decryption. Here, we show this variant. See the security proof of this scheme in the full version of [24].

5.1 Key Ideas in Constructing the Proposed IPE Scheme

We will explain key ideas in constructing the efficient IPE scheme.

First, we will show how short secret-keys and efficient decryption can be achieved in our scheme. Here, we will use a simplified (or toy) version of the proposed IPE scheme, for which the security is no more ensured in the standard model under the DLIN assumption. A ciphertext in the simplified IPE scheme consists of one vector element, $\boldsymbol{c}_1 \in \mathbb{G}^{n+1}$, and $c_2 \in \mathbb{G}_T$. A secret-key consists of one vector element, $\boldsymbol{k}^* \in \mathbb{G}^{n+1}$. Therefore, to achieve constant-size secret-keys, we have to compress $\boldsymbol{k}^* \in \mathbb{G}^{n+1}$ to a constant size in n (as long as the description of the vector $\vec{v}$ is not considered a part of the secret-key). We now employ a special

form of basis generation matrix, $X := \begin{pmatrix} \chi_0 & & & \mu'_0 \\ \chi_1 & \mu & & \mu'_1 \\ \vdots & & \ddots & \vdots \\ & & \mu & \mu'_{n-1} \\ \chi_n & & & \mu'_n \end{pmatrix}$ for a master secret-key, where $\mu, \mu'_i, \chi_i \xleftarrow{\cup} \mathbb{F}_q$ $(i = 0, \ldots, n)$ and a blank in the matrix denotes $0 \in \mathbb{F}_q$. The master secret-key is $\mathbb{B}^* := \begin{pmatrix} \boldsymbol{b}^*_0 \\ \vdots \\ \boldsymbol{b}^*_n \end{pmatrix} := \begin{pmatrix} \chi_0 G & & & \mu'_0 G \\ \chi_1 G & \mu G & & \mu'_1 G \\ \vdots & & \ddots & \vdots \\ & & \mu G & \mu'_{n-1} G \\ \chi_n G & & & \mu'_n G \end{pmatrix}$. Let a secret-key associated with $\vec{v} := (v_1, \ldots, v_n)$ be $\boldsymbol{k}^* := (1,\ \sigma\vec{v})_{\mathbb{B}^*} = \boldsymbol{b}^*_0 + \sigma(v_1\boldsymbol{b}^*_1 + \cdots + v_n\boldsymbol{b}^*_n) = ((\chi_0 + \sigma(\sum_{i=1}^n v_i\chi_i))G,\ v_1\sigma\mu G, \ldots, v_{n-1}\sigma\mu G,\ (\mu'_0 + \sigma(\sum_{i=1}^n v_i\mu'_i))G)$, where $\sigma \xleftarrow{\cup} \mathbb{F}_q$. Then, $\boldsymbol{k}^*$ can be compressed to only *three* group elements $(K^*_0 := (\chi_0 + \sigma(\sum_{i=1}^n v_i\chi_i))G,\ K^*_1 := \sigma\mu G,\ K^*_2 := (\mu'_0 + \sigma(\sum_{i=1}^n v_i\mu'_i))G)$ as well as $\vec{v}$, since $\boldsymbol{k}^*$ can be obtained by $(K^*_0, v_1K^*_1, \ldots, v_{n-1}K^*_1,\ K^*_2)$ (note that $v_iK^*_1 = v_i\sigma\mu G$ for $i = 1, \ldots, n-1$). That is, a secret-key (excluding $\vec{v}$) can be just three group elements, or the size is constant in n. Let $\mathbb{B} := (\boldsymbol{b}_i)$ be the dual orthonormal basis of $\mathbb{B}^* := (\boldsymbol{b}^*_i)$, and $\mathbb{B}$ be the (master) public key in the simplified IPE scheme. We also set a ciphertext for $\vec{x}$ as $\boldsymbol{c}_1 := (\zeta,\ \omega\vec{x})_{\mathbb{B}} = \zeta\boldsymbol{b}_0 + \omega(x_1\boldsymbol{b}_1 + \cdots + x_n\boldsymbol{b}_n)$ and $c_2 := g_T^{\zeta}m \in \mathbb{G}_T$. From the dual orthonormality of $\mathbb{B}$ and $\mathbb{B}^*$, it then holds that $e(\boldsymbol{c}_1, \boldsymbol{k}^*) = g_T^{\zeta+\omega\sigma(\vec{x}\cdot\vec{v})}$. Hence, a decryptor can compute g_T^{ζ} if and only if $\vec{x}\cdot\vec{v} = 0$, i.e., can obtain plaintext m by $c_2 \cdot e(\boldsymbol{c}_1, \boldsymbol{k}^*)^{-1}$. Since $\boldsymbol{k}^*$ is expressed as $(K^*_0, v_1K^*_1, \ldots, v_{n-1}K^*_1, K^*_2) \in \mathbb{G}^{n+1}$ and $\boldsymbol{c}_1$ is parsed as a $(n+1)$-tuple $(C_0, \ldots, C_n) \in \mathbb{G}^{n+1}$, the value of $e(\boldsymbol{c}_1, \boldsymbol{k}^*)$ is $e(C_0, K^*_0) \cdot \prod_{i=1}^{n-1} e(C_i, v_iK^*_1) \cdot e(C_n, K^*_2) = e(C_0, K^*_0) \cdot \prod_{i=1}^{n-1} e(v_iC_i, K^*_1) \cdot e(C_n, K^*_2) = e(C_0, K^*_0) \cdot e(\sum_{i=1}^{n-1} v_iC_i, K^*_1) \cdot e(C_n, K^*_2)$. That is, $n-1$ scalar multiplications in $\mathbb{G}$ and *three* pairing operations are enough for computing $e(\boldsymbol{c}_1, \boldsymbol{k}^*)$. Therefore, only a small number of pairing operations are required for decryption.

We then explain how our *full* IPE scheme is constructed on the above-mentioned simplified IPE scheme. The target of designing the full IPE scheme is to achieve the adaptively and fully attribute-hiding security under the DLIN assumption. Here, we adopt a strategy similar to that of Section 4, in which the extended dual system encryption methodology is employed in a modular or hierarchical manner. That is, two top level assumptions, the security of Problems 1, 2, and 3 are directly used in the dual system encryption methodology and these assumptions are reduced to a primitive assumption, the DLIN assumption.

To meet the requirements for applying to the extended dual system encryption methodology and reducing to the DLIN assumption, the underlying vector space as well as the basis generator matrix X is (almost) *five* times greater than that of the above-mentioned simplified scheme. For example, $\boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ 0^{2n},\ \eta\vec{v},\ 0^n\ )_{\mathbb{B}^*}$, $\boldsymbol{c}_1 = (\ \zeta,\ \omega\vec{x},\ 0^{2n},\ 0^n,\ \vec{\varphi}\ )_{\mathbb{B}}$, and $X := \begin{pmatrix} \chi_{0,0} & \chi_{0,1}\vec{e}_n & \cdots & \chi_{0,5}\vec{e}_n \\ \vec{\chi}^{\mathrm{T}}_{1,0} & X_{1,1} & \cdots & X_{1,5} \\ \vdots & \vdots & & \vdots \\ \vec{\chi}^{\mathrm{T}}_{5,0} & X_{5,1} & \cdots & X_{5,5} \end{pmatrix}$ where $\chi_{\iota,l} \xleftarrow{\cup} \mathbb{F}_q$ and each $X_{i,j}$ is of the same form as a $n \times n$ submatrix $\begin{pmatrix} \mu & & & \mu'_1 \\ & \ddots & & \vdots \\ & & \mu & \mu'_{n-1} \\ & & & \mu'_n \end{pmatrix}$ of X in the simplified scheme with $\mu, \mu'_i \xleftarrow{\cup} \mathbb{F}_q$ $(i = 1, \ldots, n)$. Using a similar technique as above, $\boldsymbol{k}^*$ can be compressed to 11 $(= 1 + 2 \times 5)$ group elements,

and $5(n-1)$ scalar multiplications in $\mathbb{G}$ and 11 pairing operations are enough for computing $e(\boldsymbol{c}_1, \boldsymbol{k}^*)$ in decryption.

5.2 Construction and Security

Let $N := 5n + 1$ and

$$\mathcal{H}(n, \mathbb{F}_q) := \left\{ \begin{pmatrix} \mu & & & \mu'_1 \\ & \ddots & & \vdots \\ & & \mu & \mu'_{n-1} \\ & & & \mu'_n \end{pmatrix} \middle| \begin{array}{l} \mu, \mu'_l \in \mathbb{F}_q \text{ for } l = 1, \ldots, n, \\ \text{a blank element in the matrix} \\ \text{denotes } 0 \in \mathbb{F}_q \end{array} \right\}, \tag{10}$$

$$\mathcal{L}^+(5, n, \mathbb{F}_q) := \left\{ X := \begin{pmatrix} \chi_{0,0} & \chi_{0,1}\vec{e}_n & \cdots & \chi_{0,5}\vec{e}_n \\ \vec{\chi}_{1,0}^{\mathrm{T}} & X_{1,1} & \cdots & X_{1,5} \\ \vdots & \vdots & & \vdots \\ \vec{\chi}_{5,0}^{\mathrm{T}} & X_{5,1} & \cdots & X_{5,5} \end{pmatrix} \middle| \begin{array}{l} X_{i,j} \in \mathcal{H}(n, \mathbb{F}_q), \\ \vec{\chi}_{i,0} := (\chi_{i,0,l})_{l=1,\ldots,n} \in \mathbb{F}_q^n, \\ \chi_{0,0}, \chi_{0,j} \in \mathbb{F}_q \\ \text{for } i, j = 1, \ldots, 5 \end{array} \right\}$$
$$\bigcap GL(N, \mathbb{F}_q). \tag{11}$$

We note that $\mathcal{L}^+(5, n, \mathbb{F}_q)$ is a subgroup of $GL(N, \mathbb{F}_q)$. Random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}$ below is used as a subroutine in the proposed IPE.

$$\begin{array}{l} \mathcal{G}_{\mathsf{ob}}^{\mathsf{ZIPE,SK}}(1^\lambda, 5, n): \quad \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),\ N := 5n + 1, \\ \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,\ g_T := e(G, G)^\psi,\ \mathsf{param}_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N, \mathsf{param}_{\mathbb{G}}), \\ \mathsf{param}_n := (\mathsf{param}_{\mathbb{V}},\ g_T),\ X \xleftarrow{\mathsf{U}} \mathcal{L}^+(5, n, \mathbb{F}_q),\ (\vartheta_{i,j})_{i,j=0,\ldots,5n} := \psi \cdot (X^{\mathrm{T}})^{-1}, \\ \text{hereafter, } \{\chi_{0,0}, \chi_{0,j}, \chi_{i,0,l}, \mu_{i,j}, \mu'_{i,j,l}\}_{i,j=1,\ldots5;l=1,\ldots,n} \text{ denotes non-zero} \\ \text{entries of } X, \text{ where } \{\mu_{i,j}, \mu'_{i,j,l}\} \text{ are non-zero entries of submatrices } X_{i,j} \text{ of} \\ X \text{ as given in Eqs. (11) and (10)}, \\ \boldsymbol{b}_i := (\vartheta_{i,0}, \ldots, \vartheta_{i,5n})_{\mathbb{A}} = \sum_{j=0}^{5n} \vartheta_{i,j}\boldsymbol{a}_j \text{ for } i = 0, \ldots, 5n,\ \mathbb{B} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{5n}), \\ B^*_{0,0} := \chi_{0,0}G, B^*_{0,j} := \chi_{0,j}G, B^*_{i,0,l} := \chi_{i,0,l}G, B^*_{i,j} := \mu_{i,j}G, B'^*_{i,j,l} := \mu'_{i,j,l}G \\ \qquad\qquad \text{for } i, j = 1, \ldots, 5; l = 1, \ldots, n, \\ \text{return } \ (\mathsf{param}_n, \mathbb{B}, \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,5;l=1,\ldots,n}). \end{array}$$

Remark 2 Let $\boldsymbol{b}^*_0 := (\ B^*_{0,0},\ 0^{n-1}, B^*_{0,1}, \ldots, 0^{n-1}, B^*_{0,5}\ )$,

$$\begin{pmatrix} \boldsymbol{b}^*_{(i-1)n+1} \\ \vdots \\ \boldsymbol{b}^*_{in} \end{pmatrix} := \begin{pmatrix} B^*_{i,0,1} & B^*_{i,1} & & & B'^*_{i,1,1} & & B^*_{i,5} & & & B'^*_{i,5,1} \\ \vdots & & \ddots & & \vdots & & & \ddots & & \vdots \\ B^*_{i,0,n-1} & & & B^*_{i,1} & B'^*_{i,1,n-1} & \cdots & & & B^*_{i,5} & B'^*_{i,5,n-1} \\ B^*_{i,0,n} & & & & B'^*_{i,1,n} & & & & & B'^*_{i,5,n} \end{pmatrix}$$

for $i = 1, \ldots, 5$, and $\mathbb{B}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{5n})$, where a blank element in the matrix denotes $0 \in \mathbb{G}$. $\mathbb{B}^*$ is the dual orthonormal basis of $\mathbb{B}$, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}^*_i) = g_T$ and $e(\boldsymbol{b}_i, \boldsymbol{b}^*_j) = 1$ for $0 \le i \ne j \le 5n$.

Here, we assume that input vector, $\vec{v} := (v_1, \ldots, v_n)$, has an index l $(1 \leq l \leq n-1)$ with $v_l \neq 0$, and that input vector, $\vec{x} := (x_1, \ldots, x_n)$, satisfies $x_n \neq 0$.

$\mathsf{Setup}(1^\lambda,\ n)$:

$(\mathsf{param}_n, \mathbb{B},\ \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i,j=1,\ldots,5;l=1,\ldots,n}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{ZIPE,SK}}_{\mathsf{ob}}(1^\lambda, 5, n)$,

$\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}, \ldots, \boldsymbol{b}_{5n})$,

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_n, \widehat{\mathbb{B}}), \mathsf{sk} := \{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i=1,4;j=1,..,5;l=1,..,n}$.

$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \vec{v})$: $\quad \sigma, \eta \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad K^*_0 := B^*_{0,0} + \sum_{l=1}^n v_l(\sigma B^*_{1,0,l} + \eta B^*_{4,0,l})$,

$K^*_{1,j} := \sigma B^*_{1,j} + \eta B^*_{4,j},\ K^*_{2,j} := B^*_{0,j} + \sum_{l=1}^n v_l(\sigma B'^*_{1,j,l} + \eta B'^*_{4,j,l})$ for $j = 1, .., 5$,

return $\mathsf{sk}_{\vec{v}} := (\vec{v}, K^*_0, \{K^*_{1,j}, K^*_{2,j}\}_{j=1,\ldots,5})$.

$\mathsf{Enc}(\mathsf{pk},\ m,\ \vec{x})$: $\quad \omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\varphi} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, \quad \boldsymbol{c}_1 := (\ \zeta,\ \overbrace{\omega\vec{x}}^{n},\ \overbrace{0^{2n}}^{2n},\ \overbrace{0^n}^{n},\ \overbrace{\vec{\varphi}}^{n}\ )_{\mathbb{B}}$,

$c_2 := g_T^\zeta m$, $\quad$ return $\mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2)$.

$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (\vec{v}, K^*_0, \{K^*_{1,j}, K^*_{2,j}\}_{j=1,\ldots,5}),\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$:

Parse $\boldsymbol{c}_1$ as a $(5n+1)$-tuple $(C_0, \ldots, C_{5n}) \in \mathbb{G}^{5n+1}$,

$D_j := \sum_{l=1}^{n-1} v_l C_{(j-1)n+l}$ for $j = 1, \ldots, 5$,

$F := e(C_0, K^*_0) \cdot \prod_{j=1}^5 \Big(e(D_j, K^*_{1,j}) \cdot e(C_{jn}, K^*_{2,j})\Big)$, $\quad$ return $m' := c_2/F$.

Remark 3 A part of output of $\mathsf{Setup}(1^\lambda, n)$, $\{B^*_{0,0}, B^*_{0,j}, B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i=1,4;j=1,\ldots,5;l=1,\ldots,n}$, can be identified with $\widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n})$, while $\mathbb{B}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_{5n})$ is identified with $\{B^*_{0,0}, B^*_{0,j},\ B^*_{i,0,l}, B^*_{i,j}, B'^*_{i,j,l}\}_{i=1,\ldots,5;j=1,\ldots,5;l=1,\ldots,n}$ in Remark 2. Decryption Dec can be alternatively described as:

$\mathsf{Dec}'(\mathsf{pk},\ \mathsf{sk}_{\vec{v}} := (\vec{v}, K^*_0, \{K^*_{1,j}, K^*_{2,j}\}_{j=1,\ldots,5}),\ \mathsf{ct}_{\vec{x}} := (\boldsymbol{c}_1, c_2))$:

$\boldsymbol{k}^* := (\overbrace{K^*_0, v_1K^*_{1,1}, .., v_{n-1}K^*_{1,1}, K^*_{2,1},}^{n} \quad \ldots, \quad \overbrace{v_1K^*_{1,5}, .., v_{n-1}K^*_{1,5}, K^*_{2,5}}^{n})$,

that is, $\boldsymbol{k}^* = (1,\ \overbrace{\sigma\vec{v},}^{n}\ \overbrace{0^{2n},}^{2n}\ \overbrace{\eta\vec{v}}^{n}\ \overbrace{0^n}^{n}\ )_{\mathbb{B}^*}$, $\quad F := e(\boldsymbol{c}_1, \boldsymbol{k}^*)$,

return $m' := c_2/F$.

Theorem 2 *The proposed IPE scheme is adaptively attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{0\text{-}1}, \mathcal{E}_{0\text{-}2}, \mathcal{E}_{1\text{-}1}, \mathcal{E}_{1\text{-}2\text{-}1}$ and $\mathcal{E}_{1\text{-}2\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) + \sum_{h=1}^{\nu} \Big(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}2\text{-}h}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}}(\lambda)\Big) + \epsilon,$$

where $\mathcal{E}_{0\text{-}2\text{-}h}(\cdot) := \mathcal{E}_{0\text{-}2}(h, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}1}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}1}(h, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}h\text{-}2}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}2}(h, \cdot)$, ν is the maximum number of $\mathcal{A}$'s key queries and $\epsilon := (29\nu + 17)/q$.

6 Comparison

Table 2 compares the proposed IPE schemes in Sections 4 and 5 with existing attribute-hiding IPE schemes in [19, 22, 20, 23].

Table 2: Comparison with IPE schemes in [19, 22, 20, 23], where $|\mathbb{G}|$ and $|\mathbb{G}_T|$ represent size of an element of $\mathbb{G}$ and that of $\mathbb{G}_T$, respectively. AH, PK, SK, CT, GSD, DSP and eDDH stand for attribute-hiding, master public key, secret key, ciphertext, general subgroup decision [1], decisional subspace problem [22], and extended decisional Diffie-Hellman [20], respectively.

	KSW08 [19]	OT09 [22]	LOS$^+$10 [20]	OT10 [23]	Proposed (basic)	Proposed (variant)
Security	selective & fully-AH	selective & weakly-AH	adaptive & weakly-AH	adaptive & weakly-AH	adaptive & fully-AH	adaptive & fully-AH
Order of $\mathbb{G}$	composite	prime	prime	prime	prime	prime
Assump.	2 variants of GSD	2 variants of DSP	n-eDDH	DLIN	DLIN	DLIN
PK size	$O(n)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n^2)\|\mathbb{G}\|$	$O(n)\|\mathbb{G}\|$
SK size	$(2n+1)\|\mathbb{G}\|$	$(n+3)\|\mathbb{G}\|$	$(2n+3)\|\mathbb{G}\|$	$(3n+2)\|\mathbb{G}\|$	$(4n+2)\|\mathbb{G}\|$	$11\|\mathbb{G}\|$
CT size	$(2n+1)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$	$(n+3)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$	$(2n+3)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$	$(3n+2)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$	$(4n+2)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$	$(5n+1)\|\mathbb{G}\|$ $+ \|\mathbb{G}_T\|$

7 Extension to HIPE

The proposed IPE scheme is extended to a hierarchical IPE (HIPE) scheme by applying the similar construction given in Appendix H.4 in the full version of [23].

7.1 Dual Orthonormal Basis Generator

We describe random dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{HIPE}}$ below, which is used as a subroutine in the proposed HIPE scheme.

$$\mathcal{G}_{\mathsf{ob}}^{\mathsf{HIPE}}(1^\lambda, \vec{n} := (d; n_1, \ldots, n_d)) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda), \quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times,$$
$$N_0 := 5, \quad N_t := 4n_t + 1 \quad \text{for } t = 1, \ldots, d,$$
$$\text{for } t = 0, \ldots, d,$$
$$\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t, \mathsf{param}_{\mathbb{G}}),$$
$$X_t := \begin{pmatrix} \vec{\chi}_{t,1} \\ \vdots \\ \vec{\chi}_{t,N_t} \end{pmatrix} := (\chi_{t,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q), \quad \begin{pmatrix} \vec{\vartheta}_{t,1} \\ \vdots \\ \vec{\vartheta}_{t,N_t} \end{pmatrix} := (\vartheta_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$$
$$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{for } i = 1, \ldots, N_t, \quad \mathbb{B}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,N_t}),$$
$$\boldsymbol{b}^*_{t,i} := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \textstyle\sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j} \quad \text{for } i = 1, \ldots, N_t, \quad \mathbb{B}^*_t := (\boldsymbol{b}^*_{t,1}, \ldots, \boldsymbol{b}^*_{t,N_t}),$$
$$g_T := e(G, G)^\psi, \quad \mathsf{param}_{\vec{n}} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d}, \ g_T)$$
$$\text{return} \quad (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d}).$$

We note that $g_T = e(\boldsymbol{b}_{t,i}, \boldsymbol{b}^*_{t,i})$ for $t = 0, \ldots, d; i = 1, \ldots, N_t$.

7.2 Special Notations for the Proposed HIPE

To express our delegation mechanisms in the HIPE compactly, we will use the same notation as in [23].

Since we use dual orthonormal basis generator $\mathcal{G}_{\mathsf{ob}}^{\mathsf{HIPE}}$, $X_0 \xleftarrow{\mathsf{U}} GL(5, \mathbb{F}_q)$ and $X_t \xleftarrow{\mathsf{U}} GL(4n_t + 1, \mathbb{F}_q)$ for $t = 1, \ldots, d$. By arranging the matrices $X_0, X_1, \ldots X_d$ diagonally and other off-diagonal parts are zero, we consider a special from of bases generation matrix $X \in \mathbb{F}_q^{N \times N}$ with $N := 5 + \sum_{t=1}^{d}(4n_t + 1)$, where

$$X := \begin{pmatrix} X_0 & & & \\ & X_1 & & \\ & & \ddots & \\ & & & X_d \end{pmatrix},$$

and our HIPEs are constructed on the one vector space $\mathbb{V}$ ($\cong \mathbb{G}^N$) with special bases induced by X. In other words, the matrix X gives direct sum decomposition $\mathbb{V} \cong \mathbb{V}_0 \oplus \mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_d$ (resp. $\mathbb{V}^* \cong \mathbb{V}_0^* \oplus \mathbb{V}_1^* \oplus \cdots \oplus \mathbb{V}_d^*$), where $\mathbb{V}_t := \mathsf{span}\langle \mathbb{B}_t \rangle$ (resp. $\mathbb{V}_t^* := \mathsf{span}\langle \mathbb{B}_t^* \rangle$) for $t = 0, \ldots, d$. Based on this isomorphism, i.e., embedding of $\mathbb{V}_t$ (resp. $\mathbb{V}_t^*$) in $\mathbb{V}$ (resp. $\mathbb{V}^*$), we define the following notations as:

$$\begin{aligned}
&((\vec{x}_0)_{\mathbb{B}_0}, \ldots, (\vec{x}_d)_{\mathbb{B}_d}) + ((\vec{y}_0)_{\mathbb{B}_0}, \ldots, (\vec{y}_d)_{\mathbb{B}_d}) := ((\vec{x}_0 + \vec{y}_0)_{\mathbb{B}_0}, \ldots, (\vec{x}_d + \vec{y}_d)_{\mathbb{B}_d}) \\
&\quad \text{where } ((\vec{x}_0)_{\mathbb{B}_0}, \ldots, (\vec{x}_d)_{\mathbb{B}_d}),\ ((\vec{y}_0)_{\mathbb{B}_0}, \ldots, (\vec{y}_d)_{\mathbb{B}_d}) \in \mathbb{V} \cong \mathbb{V}_0 \oplus \mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_d, \\
&(\vec{x})_{\mathbb{B}_t} := ((\vec{0})_{\mathbb{B}_0}, \cdots, (\vec{0})_{\mathbb{B}_{t-1}}, (\vec{x})_{\mathbb{B}_t}, (\vec{0})_{\mathbb{B}_{t+1}}, \cdots, (\vec{0})_{\mathbb{B}_d}) \in \mathbb{V}, \\
&((\vec{x}_0)_{\mathbb{B}_0}, (\vec{x}_t)_{\mathbb{B}_t} : t = 1, \ldots, \ell) := ((\vec{x}_0)_{\mathbb{B}_0}, \ldots, (\vec{x}_\ell)_{\mathbb{B}_\ell}) := \textstyle\sum_{t=0}^{\ell} (\vec{x}_t)_{\mathbb{B}_t} \in \mathbb{V}, \\
&((\vec{x}_0)_{\mathbb{B}_0}, (\vec{x}_t)_{\mathbb{B}_t} : t = 1, \ldots, \ell, (\vec{x}_\tau)_{\mathbb{B}_\tau}) := ((\vec{x}_0)_{\mathbb{B}_0}, \ldots, (\vec{x}_\ell)_{\mathbb{B}_\ell}, (\vec{x}_\tau)_{\mathbb{B}_\tau}) \\
&\qquad\qquad := \textstyle\sum_{t=0,\ldots,\ell,\tau} (\vec{x}_t)_{\mathbb{B}_t} \in \mathbb{V}, \\
&e(\boldsymbol{c}, \boldsymbol{k}^*) := \textstyle\prod_{t=0}^{d} e(\boldsymbol{c}_t, \boldsymbol{k}_t^*) \quad \text{where } \boldsymbol{c} := (\boldsymbol{c}_0, \ldots, \boldsymbol{c}_d) \in \mathbb{V}_0 \oplus \cdots \oplus \mathbb{V}_d, \\
&\qquad\qquad \boldsymbol{k}^* := (\boldsymbol{k}_0^*, \ldots, \boldsymbol{k}_d^*) \in \mathbb{V}_0^* \oplus \cdots \oplus \mathbb{V}_d^*, \\
&\text{and } \ \vec{e}_{t,j} := (\overbrace{0, \ldots, 0}^{j-1}, 1, \overbrace{0, \ldots, 0}^{n_t - j}) \in \mathbb{F}_q^{n_t},
\end{aligned}$$

and all the above notations are applied to the case with $\{\mathbb{B}_t^*\}_{t=0,\ldots,d}$ instead of $\{\mathbb{B}_t\}_{t=0,\ldots,d}$

7.3 Construction

In the description of the scheme, we assume that the first coordinates, $x_{i,1}$, of input vectors, $\vec{x}_i := (x_{i,1}, \ldots, x_{i,n_i})$ for $i = 1, \ldots, \ell$, are nonzero.

$\mathsf{Setup}(1^\lambda,\ \vec{n} := (d; n_1, \ldots, n_d)) :\quad (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{HIPE}}(1^\lambda, \vec{n})$,

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,3}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, .., \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,4n_t+1})$ for $t = 1, .., d$,

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,3}^*)$, $\widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, .., \boldsymbol{b}_{t,n_t}^*)$ for $t = 1, .., d$,

return $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \boldsymbol{b}_{0,4}^*, \{\boldsymbol{b}_{t,3n_t+1}^*, .., \boldsymbol{b}_{t,4n_t}^*\}_{t=1,\ldots,d})$, $\mathsf{sk} := \{\widehat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}$.

$\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, (\vec{v}_1, \ldots, \vec{v}_\ell) \in \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_\ell}) :$

for $j = 1, \ldots, 2\ell;\ \tau = \ell + 1, \ldots, d;\ \iota = 1, \ldots, n_\tau$;

$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},1,j,t}, \theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},1,j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, \ell$,

$s_{\mathsf{del},(\tau,\iota),t}, s_{\mathsf{ran},2,\tau,t}, \theta_{\mathsf{del},(\tau,\iota),t}, \theta_{\mathsf{ran},2,\tau,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $t = 1, \ldots, \ell + 1$,

$s_{\mathsf{dec},0} := \sum_{t=1}^{\ell} s_{\mathsf{dec},t}$, $s_{\mathsf{del},(\tau,\iota),0} := \sum_{t=1}^{\ell+1} s_{\mathsf{del},(\tau,\iota),t}$,

$s_{\mathsf{ran},1,j,0} := \sum_{t=1}^{\ell} s_{\mathsf{ran},1,j,t}$, $s_{\mathsf{ran},2,\tau,0} := \sum_{t=1}^{\ell+1} s_{\mathsf{ran},2,\tau,t}$,

$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},1,j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$ for $t = 0, \ldots, \ell$,

$\vec{\eta}_{\mathsf{del},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{ran},2,\tau,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}$, for $t = 0, \ldots, \ell+1$,

$\boldsymbol{k}^*_{\ell,\mathsf{dec}} := \quad (\ (\ -s_{\mathsf{dec},0},\ 0,\ 1,\ \eta_{\mathsf{dec},0},\ 0\ )_{\mathbb{B}^*_0},$

$(\ s_{\mathsf{dec},t}\vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t, \quad 0^{2n_t}, \quad \vec{\eta}_{\mathsf{dec},t},\ 0\ )_{\mathbb{B}^*_t} : t = 1, \ldots, \ell),$

$\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)} := (\ (\ -s_{\mathsf{del},(\tau,\iota),0},\ 0,\ 0,\ \eta_{\mathsf{del},(\tau,\iota),0},\ 0\ )_{\mathbb{B}^*_0},$

$(\ s_{\mathsf{del},(\tau,\iota),t}\vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{2n_t}, \quad \vec{\eta}_{\mathsf{del},(\tau,\iota),t},\ 0\ )_{\mathbb{B}^*_t} : t = 1, \ldots, \ell,$

$(\ s_{\mathsf{del},(\tau,\iota),\ell+1}\vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, \quad 0^{2n_\tau}, \quad \vec{\eta}_{\mathsf{del},(\tau,\iota),\ell+1},\ 0\ )_{\mathbb{B}^*_\tau}),$

$\boldsymbol{k}^*_{\ell,\mathsf{ran},1,j} := (\ (\ -s_{\mathsf{ran},1,j,0},\ 0,\ 0,\ \eta_{\mathsf{ran},1,j,0},\ 0\ )_{\mathbb{B}^*_0},$

$(\ s_{\mathsf{ran},1,j,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},1,j,t}\vec{v}_t, \quad 0^{2n_t}, \quad \vec{\eta}_{\mathsf{ran},1,j,t},\ 0\ )_{\mathbb{B}^*_t} : t = 1, \ldots, \ell),$

$\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau} := (\ (\ -s_{\mathsf{ran},2,\tau,0},\ 0,\ 0,\ \eta_{\mathsf{ran},2,\tau,0},\ 0\ )_{\mathbb{B}^*_0},$

$(\ s_{\mathsf{ran},2,\tau,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},2,\tau,t}\vec{v}_t, \quad 0^{2n_t}, \quad \vec{\eta}_{\mathsf{ran},2,\tau,t},\ 0\ )_{\mathbb{B}^*_t} : t = 1, \ldots, \ell,$

$(\ s_{\mathsf{ran},2,\tau,\ell+1}\vec{e}_{\tau,1}, \quad 0^{2n_\tau}, \quad \vec{\eta}_{\mathsf{ran},2,\tau,\ell+1},\ 0\ )_{\mathbb{B}^*_\tau}),$

$\mathsf{sk}_\ell := (\boldsymbol{k}^*_{\ell,\mathsf{dec}}, \{\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)}\}_{\tau=\ell+1,\ldots,d;\ \iota=1,\ldots,n_\tau}, \{\boldsymbol{k}^*_{\ell,\mathsf{ran},1,j},\ \boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau}\}_{j=1,\ldots,2\ell;\ \tau=\ell+1,\ldots,d})$,

return sk_ℓ.

$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1, \ldots, \vec{x}_\ell) \in \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_\ell})$:

$\omega, \varphi_0, \ldots, \varphi_\ell \xleftarrow{\mathsf{U}} \mathbb{F}_q, \quad \boldsymbol{c}_1 := (\ (\omega, 0, \zeta, 0, \varphi_0)_{\mathbb{B}_0},\ (\omega\vec{x}_t, 0^{2n_t}, 0^{n_t}, \varphi_t)_{\mathbb{B}_t} : t = 1, \ldots, \ell),$

$c_2 := g_T^\zeta m, \qquad \mathsf{ct} := (\boldsymbol{c}_1, c_2), \quad$ return ct.

$\mathsf{Dec}(\mathsf{pk}, \boldsymbol{k}^*_{\ell,\mathsf{dec}}, \mathsf{ct})$: $m' := c_2/e(\boldsymbol{c}_1, \boldsymbol{k}^*_{\ell,\mathsf{dec}}), \quad$ return m'.

$\mathsf{Delegate}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, \vec{v}_{\ell+1} := (v_{\ell+1,1}, \ldots, v_{\ell+1,n_{\ell+1}}))$:

for $j' = 1, \ldots, 2(\ell+1);\ \tau = \ell+2, \ldots, d;\ \iota = 1, \ldots, n_\tau$;

$\phi_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{ran},2,\tau},\ \psi' \xleftarrow{\mathsf{U}} \mathbb{F}_q,$

$\boldsymbol{p}^*_{\mathsf{dec}}, \boldsymbol{p}^*_{\mathsf{del},(\tau,\iota)}, \boldsymbol{p}^*_{\mathsf{ran},1,j'}, \boldsymbol{p}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{R}} \mathsf{CoreDel}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, \vec{v}_{\ell+1})$,

where $\mathsf{CoreDel}_\ell(\mathsf{pk}, \mathsf{sk}_\ell, \vec{v}_{\ell+1})$: $\sigma, \alpha_j \xleftarrow{\mathsf{U}} \mathbb{F}_q$ for $j = 1, \ldots, 2\ell+1$,

return $\boldsymbol{p}^* := \sigma(\sum_{i=1}^{n_{\ell+1}} v_{\ell+1,i}\boldsymbol{k}^*_{\ell,\mathsf{del},(\ell+1,i)}) + \sum_{j=1}^{2\ell} \alpha_j \boldsymbol{k}^*_{\ell,\mathsf{ran},1,j} + \alpha_{2\ell+1}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\ell+1}$,

$\boldsymbol{r}^*_{\mathsf{dec}}, \boldsymbol{r}^*_{\mathsf{ran},1,j'} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{0,4}, \{\boldsymbol{b}^*_{t,3n_t+i}\}_{t=1,\ldots,\ell+1;\ i=1,\ldots,n_t}\rangle,$

$\boldsymbol{r}^*_{\mathsf{del},(\tau,\iota)}, \boldsymbol{r}^*_{\mathsf{ran},2,\tau} \xleftarrow{\mathsf{U}} \mathsf{span}\langle \boldsymbol{b}^*_{0,4}, \{\boldsymbol{b}^*_{t,3n_t+i}\}_{t=1,\ldots,\ell+1,\tau;\ i=1,\ldots,n_t}\rangle,$

$\boldsymbol{k}^*_{\ell+1,\mathsf{dec}} := \boldsymbol{k}^*_{\ell,\mathsf{dec}} + \boldsymbol{p}^*_{\mathsf{dec}} + \boldsymbol{r}^*_{\mathsf{dec}},$

$\boldsymbol{k}^*_{\ell+1,\mathsf{del},(\tau,\iota)} := \boldsymbol{p}^*_{\mathsf{del},(\tau,\iota)} + \phi_{\mathsf{del},(\tau,\iota)}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau} + \psi'\boldsymbol{k}^*_{\ell,\mathsf{del},(\tau,\iota)} + \boldsymbol{r}^*_{\mathsf{del},(\tau,\iota)},$

$\boldsymbol{k}^*_{\ell+1,\mathsf{ran},1,j'} := \boldsymbol{p}^*_{\mathsf{ran},1,j'} + \boldsymbol{r}^*_{\mathsf{ran},1,j'},$

$\boldsymbol{k}^*_{\ell+1,\mathsf{ran},2,\tau} := \boldsymbol{p}^*_{\mathsf{ran},2,\tau} + \phi_{\mathsf{ran},2,\tau}\boldsymbol{k}^*_{\ell,\mathsf{ran},2,\tau} + \boldsymbol{r}^*_{\mathsf{ran},2,\tau},$

$\mathsf{sk}_{\ell+1} := (\boldsymbol{k}^*_{\ell+1,\mathsf{dec}}, \{\boldsymbol{k}^*_{\ell+1,\mathsf{del},(\tau,\iota)}\}_{\tau=\ell+2,\ldots,d;\ \iota=1,\ldots,n_\tau},$

$\{\boldsymbol{k}^*_{\ell+1,\mathsf{ran},1,j'}, \boldsymbol{k}^*_{\ell+1,\mathsf{ran},2,\tau}\}_{j'=1,\ldots,2(\ell+1);\ \tau=\ell+2,\ldots,d})$,

return $\mathsf{sk}_{\ell+1}$.

Lemma 13 shows the distribution of delegated keys and that of the corresponding freshly-generated keys are equivalent (except with negligible probability).

Lemma 13 *If* sk_ℓ *is generated by* $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, (\vec{v}_1, \ldots, \vec{v}_\ell))$*, the distribution of* $\mathsf{sk}_{\ell+1}$ *generated by* $\mathsf{Delegate}(\mathsf{pk}, \mathsf{sk}_\ell, \vec{v}_{\ell+1})$ *is equivalent to that of* $\mathsf{sk}_{\ell+1}$ *generated by* $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{sk}, (\vec{v}_1, \ldots, \vec{v}_\ell, \vec{v}_{\ell+1}))$ *except with probability at most* $(2d - 2\ell + 3)/q$.

Lemma 13 is proven in the same manner as that in the full version of [23].

7.4 Security

Theorem 3 *The proposed HIPE scheme is adaptively (fully) attribute-hiding against chosen plaintext attacks under the DLIN assumption.*

For any adversary $\mathcal{A}$, there exist probabilistic machines $\mathcal{E}_{0\text{-}1}, \mathcal{E}_{0\text{-}2}, \mathcal{E}_{1\text{-}1}, \mathcal{E}_{1\text{-}2\text{-}1}$ and $\mathcal{E}_{1\text{-}2\text{-}2}$, whose running times are essentially the same as that of $\mathcal{A}$, such that for any security parameter λ,

$$\begin{aligned}\mathsf{Adv}^{\mathsf{HIPE,AH}}_{\mathcal{A}}(\lambda) &\leq \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}1}}(\lambda) \\ &+ \sum_{h=1}^{\nu}\sum_{I=1}^{L}\left(\mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{0\text{-}2\text{-}(h,I)}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}(h,I)\text{-}1}}(\lambda) + \mathsf{Adv}^{\mathsf{DLIN}}_{\mathcal{E}_{1\text{-}2\text{-}(h,I)\text{-}2}}(\lambda)\right) + \epsilon,\end{aligned}$$

where $\mathcal{E}_{0\text{-}2\text{-}(h,I)}(\cdot) := \mathcal{E}_{0\text{-}2}(h, I, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}(h,I)\text{-}1}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}1}(h, I, \cdot)$, $\mathcal{E}_{1\text{-}2\text{-}(h,I)\text{-}2}(\cdot) := \mathcal{E}_{1\text{-}2\text{-}2}(h, I, \cdot)$, ν is the maximum number of $\mathcal{A}$'s key queries, $L := d{+}2{+}\sum_{\tau=2}^{d} n_\tau$, and $\epsilon := ((2d{+}33)L\nu{+}6d{+}23)/q$.

The weakly attribute-hiding security of HIPE in the full version of [23] implies the security of our HIPE with $t = 0$ as in Theorem 1, and the security with $t = 1$ is proven in a similar manner as Lemma 1.

References

[1] Mihir Bellare, Brent Waters, and Scott Yilek. Identity-based encryption secure against selective opening attack. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 235–252. Springer, 2011.

[2] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society, 2007.

[3] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In Cachin and Camenisch [12], pages 223–238.

[4] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Franklin [16], pages 443–459.

[5] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Cramer [15], pages 440–456.

[6] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Franklin [16], pages 41–55.

[7] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In Cachin and Camenisch [12], pages 506–522.

[8] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.

[9] Dan Boneh and Michael Hamburg. Generalized identity based and broadcast encryption schemes. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 455–470. Springer, 2008.

[10] Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 535–554. Springer, 2007.

[11] Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 290–307. Springer, 2006.

[12] Christian Cachin and Jan Camenisch, editors. *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *LNCS*. Springer, 2004.

[13] Angelo De Caro, Vincenzo Iovino, and Giuseppe Persiano. Hidden vector encryption fully secure against unrestricted queries. *IACR Cryptology ePrint Archive*, 2011:546, 2011.

[14] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *IMA Int. Conf. 2001*, volume 2260 of *LNCS*, pages 360–363. Springer, 2001.

[15] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *LNCS*. Springer, 2005.

[16] Matthew K. Franklin, editor. *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *LNCS*. Springer, 2004.

[17] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Juels et al. [18], pages 89–98.

[18] Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors. *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006*. ACM, 2006.

[19] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162. Springer, 2008.

[20] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *EUROCRYPT 2008*, volume 6110 of *LNCS*, pages 62–91. Springer, 2010. Full version is available at `http://eprint.iacr.org/2010/110`.

[21] Tatsuaki Okamoto and Katsuyuki Takashima. Homomorphic encryption and signatures from vector decomposition. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing 2008*, volume 5209 of *LNCS*, pages 57–74. Springer, 2008.

[22] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, 2009.

[23] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, 2010. Full version is available at `http://eprint.iacr.org/2010/563`.

[24] Tatsuaki Okamoto and Katsuyuki Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *CANS 2011*, volume 7092 of *LNCS*, pages 138–159. Springer, 2011. Full version is available at `http://eprint.iacr.org/2011/648`.

[25] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM Conference on Computer and Communications Security*, pages 195–203. ACM, 2007.

[26] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure attribute-based systems. In Juels et al. [18], pages 99–112.

[27] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Cramer [15], pages 457–473.

[28] Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP (2) 2008*, volume 5126 of *LNCS*, pages 560–578. Springer, 2008.

[29] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, 2009.

A Some Key Techniques on DPVS

A.1 Summary

We now briefly explain our approach, DPVS, constructed on symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$, where q is a prime, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order q, G is a generator of $\mathbb{G}$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear pairing operation, and $e(G, G) \neq 1$. Here we denote the group operation of $\mathbb{G}$ by addition and $\mathbb{G}_T$ by multiplication, respectively. Note that this construction also works on *asymmetric* pairing groups (in this paper, we use symmetric pairing groups for simplicity of description).

Vector space $\mathbb{V}$: $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$, whose element is expressed by N-dimensional vector, $\boldsymbol{x} := (x_1 G, \ldots, x_N G)$ ($x_i \in \mathbb{F}_q$ for $i = 1, \ldots, N$).

Canonical base $\mathbb{A}$: $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ of $\mathbb{V}$, where $\boldsymbol{a}_1 := (G, 0, \ldots, 0), \boldsymbol{a}_2 := (0, G, 0, \ldots, 0)$, $\ldots, \boldsymbol{a}_N := (0, \ldots, 0, G)$.

Pairing operation: $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(x_i G, y_i G) = e(G, G)^{\sum_{i=1}^{N} x_i y_i} = e(G, G)^{\vec{x} \cdot \vec{y}} \in \mathbb{G}_T$, where $\boldsymbol{x} := (x_1 G, \ldots, x_N G) = x_1 \boldsymbol{a}_1 + \cdots + x_N \boldsymbol{a}_N \in \mathbb{V}$, $\boldsymbol{y} := (y_1 G, \ldots, y_N G) = y_1 \boldsymbol{a}_1 + \cdots + y_N \boldsymbol{a}_N \in \mathbb{V}$, $\vec{x} := (x_1, \ldots, x_N)$ and $\vec{y} := (y_1, \ldots, y_N)$. Here, $\boldsymbol{x}$ and $\boldsymbol{y}$ can be expressed by coefficient vector over basis $\mathbb{A}$ such that $(x_1, \ldots, x_N)_{\mathbb{A}} = (\vec{x})_{\mathbb{A}} := \boldsymbol{x}$ and $(y_1, \ldots, y_N)_{\mathbb{A}} = (\vec{y})_{\mathbb{A}} := \boldsymbol{y}$.

Base change: Canonical basis $\mathbb{A}$ is changed to basis $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$ of $\mathbb{V}$ using a uniformly chosen (regular) linear transformation, $X := (\chi_{i,j}) \xleftarrow{\cup} GL(N, \mathbb{F}_q)$, such that $\boldsymbol{b}_i =$

$\sum_{j=1}^{N} \chi_{i,j}\boldsymbol{a}_j$, $(i = 1, \ldots, N)$. $\mathbb{A}$ is also changed to basis $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$ of $\mathbb{V}$, such that $(\vartheta_{i,j}) := (X^T)^{-1}$, $\boldsymbol{b}_i^* = \sum_{j=1}^{N} \vartheta_{i,j}\boldsymbol{a}_j$, $(i = 1, \ldots, N)$. We see that $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = e(G, G)^{\delta_{i,j}}$, ($\delta_{i,j} = 1$ if $i = j$, and $\delta_{i,j} = 0$ if $i \neq j$) i.e., $\mathbb{B}$ and $\mathbb{B}^*$ are dual orthonormal bases of $\mathbb{V}$.

Here, $\boldsymbol{x} := x_1\boldsymbol{b}_1 + \cdots + x_N\boldsymbol{b}_N \in \mathbb{V}$ and $\boldsymbol{y} := y_1\boldsymbol{b}_1^* + \cdots + y_N\boldsymbol{b}_N^* \in \mathbb{V}$ can be expressed by coefficient vectors over $\mathbb{B}$ and $\mathbb{B}^*$ such that $(x_1, \ldots, x_N)_{\mathbb{B}} = (\vec{x})_{\mathbb{B}} := \boldsymbol{x}$ and $(y_1, \ldots, y_N)_{\mathbb{B}^*} = (\vec{y})_{\mathbb{B}^*} := \boldsymbol{y}$, and $e(\boldsymbol{x}, \boldsymbol{y}) = e(G, G)^{\sum_{i=1}^{N} x_i y_i} = e(G, G)^{\vec{x}\cdot\vec{y}} \in \mathbb{G}_T$.

Intractable problem: One of the most natural decisional problems in this approach is the decisional subspace problem [21]. It is to tell $\boldsymbol{v} := v_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + v_{N_1}\boldsymbol{b}_{N_1}$ $(= (0, \ldots, 0, v_{N_2+1}, \ldots, v_{N_1})_{\mathbb{B}})$, from $\boldsymbol{u} := v_1\boldsymbol{b}_1 + \cdots + v_{N_1}\boldsymbol{b}_{N_1}$ $(= (v_1, \ldots, v_{N_1})_{\mathbb{B}})$, where $(v_1, \ldots, v_{N_1}) \xleftarrow{\cup} \mathbb{F}_q^{N_1}$ and $N_2 + 1 < N_1$.

Trapdoor: Although the decisional subspace problem is assumed to be intractable, it can be efficiently solved by using *trapdoor* $\boldsymbol{t}^* \in \mathsf{span}\langle \boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_{N_2}^* \rangle$. Given $\boldsymbol{v} := v_{N_2+1}\boldsymbol{b}_{N_2+1} + \cdots + v_{N_1}\boldsymbol{b}_{N_1}$ or $\boldsymbol{u} := v_1\boldsymbol{b}_1 + \cdots + v_{N_1}\boldsymbol{b}_{N_1}$, we can tell $\boldsymbol{v}$ from $\boldsymbol{u}$ using $\boldsymbol{t}^*$ since $e(\boldsymbol{v}, \boldsymbol{t}^*) = 1$ and $e(\boldsymbol{u}, \boldsymbol{t}^*) \neq 1$ with high probability.

Advantage of this approach: Higher dimensional vector treatment of bilinear pairing groups have been already employed in literature especially in the areas of IBE, ABE and BE (e.g., [5, 2, 9, 11, 17, 27]). For example, in a typical vector treatment, two vector forms of $P := (x_1G, \ldots, x_NG)$ and $Q := (y_1G, \ldots, y_NG)$ are set and pairing for P and Q is operated as $e(P, Q) := \prod_{i=1}^{N} e(x_iG, y_iG)$. Such treatment can be rephrased in this approach such that $P = x_1\boldsymbol{a}_1 + \cdots + x_N\boldsymbol{a}_N$ $(= (x_1, \ldots, x_N)_{\mathbb{A}})$, and $Q = y_1\boldsymbol{a}_1 + \cdots + y_N\boldsymbol{a}_N$ $(= (y_1, \ldots, y_N)_{\mathbb{A}})$ over canonical basis $\mathbb{A}$.

The major drawback of this approach is the easily *decomposable* property over $\mathbb{A}$ (i.e., the decisional subspace problem is easily solved). That is, it is easy to decompose $x_i\boldsymbol{a}_i = (0, \ldots, 0, x_iG, 0, \ldots, 0)$ from $P := x_1\boldsymbol{a}_1 + \cdots x_N\boldsymbol{a}_N = (x_1G, \ldots, x_NG)$.

In contrast, our approach employs basis $\mathbb{B}$, which is linearly transformed from $\mathbb{A}$ using a secret random matrix $X \in \mathbb{F}_q^{n\times n}$. A remarkable property over $\mathbb{B}$ is that it seems hard to decompose $x_i\boldsymbol{b}_i$ from $P' := x_1\boldsymbol{b}_1 + \cdots x_N\boldsymbol{b}_N$ (and the decisional subspace problem seems intractable). In addition, the secret matrix X (and the dual orthonormal basis $\mathbb{B}^*$ of $\mathbb{V}$) can be used as a source of the trapdoors to the decomposability (and distinguishability for the decisional subspace problem through the pairing operation over $\mathbb{B}$ and $\mathbb{B}^*$ as mentioned above). The hard decomposability (and indistinguishability) and its trapdoors are ones of the key tricks in this paper. Note that composite order pairing groups are often employed with similar tricks such as hard decomposability (and indistinguishability) of a composite order group to the prime order subgroups and its trapdoors through factoring (e.g., [19, 28]).

A.2 Dual Pairing Vector Spaces by Direct Product of Asymmetric Pairing Groups

Definition 11 *"Asymmetric bilinear pairing groups"* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *are a tuple of a prime* q*, cyclic additive groups* $\mathbb{G}_1, \mathbb{G}_2$ *and multiplicative group* $\mathbb{G}_T$ *of order* q*,* $G_1 \neq 0 \in \mathbb{G}_1, G_2 \neq 0 \in \mathbb{G}_2$*, and a polynomial-time computable nondegenerate bilinear pairing* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ *i.e.,* $e(sG_1, tG_2) = e(G_1, G_2)^{st}$ *and* $e(G_1, G_2) \neq 1$*.*

Let $\mathcal{G}_{\mathsf{bpg}}$ *be an algorithm that takes input* 1^λ *and outputs a description of bilinear pairing groups* $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *with security parameter* λ*.*

Definition 12 *"Dual pairing vector spaces (DPVS)"* $(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$ *by direct product of asymmetric pairing groups* $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, e)$ *are a tuple of a prime* q*, two* N*-dimensional vector spaces* $\mathbb{V} := \overbrace{\mathbb{G}_1 \times \cdots \times \mathbb{G}_1}^{N}$ *and* $\mathbb{V}^* := \overbrace{\mathbb{G}_2 \times \cdots \times \mathbb{G}_2}^{N}$ *over* $\mathbb{F}_q$*, a cyclic group* $\mathbb{G}_T$ *of order* q*, and their canonical bases i.e.,* $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$ *of* $\mathbb{V}$ *and* $\mathbb{A}^* := (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_N^*)$ *of* $\mathbb{V}^*$*, where* $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G_1, \overbrace{0, \ldots, 0}^{N-i})$ *and* $\boldsymbol{a}_i^* := (\overbrace{0, \ldots, 0}^{i-1}, G_2, \overbrace{0, \ldots, 0}^{N-i})$ *with the following operations:*

1. *[Non-degenerate bilinear pairing] The pairing on* $\mathbb{V}$ *and* $\mathbb{V}^*$ *is defined by* $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(D_i, H_i) \in \mathbb{G}_T$ *where* $(D_1, \ldots, D_N) := \boldsymbol{x} \in \mathbb{V}$ *and* $(H_1, \ldots, H_N) := \boldsymbol{y} \in \mathbb{V}^*$*. This is non-degenerate bilinear i.e.,* $e(s\boldsymbol{x}, t\boldsymbol{y}) = e(\boldsymbol{x}, \boldsymbol{y})^{st}$ *and if* $e(\boldsymbol{x}, \boldsymbol{y}) = 1$ *for all* $\boldsymbol{y} \in \mathbb{V}$*, then* $\boldsymbol{x} = \boldsymbol{0}$*. For all* i *and* j*,* $e(\boldsymbol{a}_i, \boldsymbol{a}_j^*) = g_T^{\delta_{i,j}}$ *where* $\delta_{i,j} = 1$ *if* $i = j$*, and* 0 *otherwise, and* $e(G_1, G_2) \neq 1 \in \mathbb{G}_T$*.*

2. *[Canonical maps] Linear transformation* $\phi_{i,j}$ *on* $\mathbb{V}$ *s.t.* $\phi_{i,j}(\boldsymbol{a}_j) = \boldsymbol{a}_i$ *and* $\phi_{i,j}(\boldsymbol{a}_k) = \boldsymbol{0}$ *if* $k \neq j$ *can be easily achieved by* $\phi_{i,j}(\boldsymbol{x}) := (\overbrace{0, \ldots, 0}^{i-1}, D_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $(D_1, \ldots, D_N) := \boldsymbol{x}$*. Moreover, linear transformation* $\phi_{i,j}^*$ *on* $\mathbb{V}^*$ *s.t.* $\phi_{i,j}^*(\boldsymbol{a}_j^*) = \boldsymbol{a}_i^*$ *and* $\phi_{i,j}^*(\boldsymbol{a}_k^*) = \boldsymbol{0}$ *if* $k \neq j$ *can be easily achieved by* $\phi_{i,j}^*(\boldsymbol{y}) := (\overbrace{0, \ldots, 0}^{i-1}, H_j, \overbrace{0, \ldots, 0}^{N-i})$ *where* $(H_1, \ldots, H_N) := \boldsymbol{y}$*. We call* $\phi_{i,j}$ *and* $\phi_{i,j}^*$ *"canonical maps".*

DPVS generation algorithm $\mathcal{G}_{\mathsf{dpvs}}$ *takes input* 1^λ *(*$\lambda \in \mathbb{N}$*),* $N \in \mathbb{N}$ *and a description of bilinear pairing groups* $\mathsf{param}_{\mathbb{G}}$*, and outputs a description of* $\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*, e)$ *constructed above with security parameter* λ *and* N*-dimensional* $(\mathbb{V}, \mathbb{V}^*)$*.*

B Proofs of Lemmas 4, 6–11 in Section 4.3

Proof of Lemma 4

Lemma 4 *For any adversary* $\mathcal{B}$*, there is a probabilistic machine* $\mathcal{E}$*, whose running time is essentially the same as that of* $\mathcal{B}$*, such that for any security parameter* λ*,* $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda) \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 8/q$*.*

Proof. Problem 3 is the hybrid of the following Experiment 3-0, 3-1 and 3-2, i.e., $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda) = \left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-0}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-2}}(\lambda) \to 1\right]\right|$. Therefore, from Lemmas 14, 15 and 3, there exist probabilistic machines $\mathcal{C}$ and $\mathcal{E}$, whose running time are essentially the same as that of $\mathcal{B}$, such that for any security parameter λ,

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{B}}^{\mathsf{P3}}(\lambda) &= \left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-0}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-2}}(\lambda) \to 1\right]\right| \\
&\leq \left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-0}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-1}}(\lambda) \to 1\right]\right| \\
&\quad + \left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-1}}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{\text{3-2}}(\lambda) \to 1\right]\right| \\
&\leq \mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda) + 3/q \leq \mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) + 8/q.
\end{aligned}$$

This completes the proof of Lemma 4. □

Definition 13 (Experiment 3-α ($\alpha = 0, 1, 2$)) *We define Exp-3-*α *instance generator,*

$\mathcal{G}_\alpha^{\mathsf{Exp\text{-}3}}(1^\lambda, n)$, *where*

$$
\begin{array}{l}
\mathcal{G}_\alpha^{\mathsf{Exp\text{-}3}}(1^\lambda, n): \quad (\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}^{\mathsf{IPE}}(1^\lambda, 4n+2), \\
\quad \widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{b}_{2n+1}^*, \ldots, \boldsymbol{b}_{4n+1}^*), \\
\quad \tau, \tau', \delta_0, \omega', \omega'', \kappa', \kappa'' \xleftarrow{\mathsf{U}} \mathbb{F}_q, \\
\quad \text{for } i = 1, \ldots, n; \\
\qquad\qquad \overbrace{\qquad}^{n+1} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{1} \\
\quad \boldsymbol{h}_{0,i}^* := \ (\ 0^{n+1}, \quad \tau\vec{e}_i, \quad 0^{n_t}, \quad \delta_0\vec{e}_i, \quad 0 \ )_{\mathbb{B}^*} \\
\quad \boldsymbol{h}_{1,i}^* := \ (\ 0^{n+1}, \quad \tau\vec{e}_i, \quad \tau'\vec{e}_i, \quad \delta_0\vec{e}_i, \quad 0 \ )_{\mathbb{B}^*} \\
\quad \boldsymbol{h}_{2,i}^* := \ (\ 0^{n+1}, \quad 0^{n}, \quad \tau'\vec{e}_i, \quad \delta_0\vec{e}_i, \quad 0 \ )_{\mathbb{B}^*} \\
\quad \boldsymbol{e}_i := \ (\ 0^{n+1}, \quad \omega'\vec{e}_i, \quad \omega''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{B}}, \\
\quad \boldsymbol{f}_i := \ (\ 0^{n+1}, \quad \kappa'\vec{e}_i, \quad \kappa''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{B}}, \\
\quad \text{return } (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}_{\alpha,i}^*, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n}).
\end{array}
$$

For a probabilistic adversary $\mathcal{B}$, we define 3 experiments $\mathsf{Exp}_{\mathcal{B}}^{3\text{-}\alpha}$ ($\alpha = 0, 1, 2$) as follows:

1. *$\mathcal{C}$ is given $\varrho \xleftarrow{\mathsf{R}} \mathcal{G}_\alpha^{\mathsf{Exp\text{-}3}}(1^\lambda, n)$.*
2. *Output $\beta' \xleftarrow{\mathsf{R}} \mathcal{B}(1^\lambda, \varrho)$.*

Lemma 14 *For any adversary $\mathcal{B}$, for any security parameter λ,*
$|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}0}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}1}(\lambda) \to 1\right]| \leq 1/q$.

Proof. Let $\theta \xleftarrow{\mathsf{U}} \mathbb{F}_q$. If we set

$$\boldsymbol{d}_{2n+i} := \boldsymbol{b}_{2n+i} - \theta\boldsymbol{b}_{n+i} \quad \boldsymbol{d}_{n+i}^* := \boldsymbol{b}_{n+i}^* + \theta\boldsymbol{b}_{2n+i}^* \quad \text{for } i = 1, \ldots, n.$$

Then, $\mathbb{D} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{2n}, \boldsymbol{d}_{2n+1}, \ldots, \boldsymbol{d}_{3n}, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1})$ and $\mathbb{D}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{d}_{n+1}^*, \ldots, \boldsymbol{d}_{2n}^*, \boldsymbol{b}_{2n+1}^*, \ldots, \boldsymbol{b}_{4n+1}^*)$ are dual orthonormal bases. Moreover, $(\mathbb{D}, \mathbb{D}^*)$ are consistent with $(\widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*)$. Then,

$$
\begin{array}{rl}
\qquad\qquad \overbrace{\qquad}^{n+1} & \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{n} \quad \overbrace{\qquad}^{1} \\
\boldsymbol{h}_{0,i}^* := \ (\ 0^{n+1}, & \tau\vec{e}_i, \quad 0^{n}, \quad \delta_0\vec{e}_i, \quad 0 \ )_{\mathbb{B}^*} \\
= \ (\ 0^{n+1}, & \tau\vec{e}_i, \quad \tau'\vec{e}_i, \quad \delta_0\vec{e}_i, \quad 0 \ )_{\mathbb{D}^*} \\
\boldsymbol{e}_i := \ (\ 0^{n+1}, & \omega'\vec{e}_i, \quad \omega''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{B}}, \\
= \ (\ 0^{n+1}, & \widetilde{\omega}'\vec{e}_i, \quad \omega''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{D}}, \\
\boldsymbol{f}_i := \ (\ 0^{n+1}, & \kappa'\vec{e}_i, \quad \kappa''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{B}}, \\
= \ (\ 0^{n+1}, & \widetilde{\kappa}'\vec{e}_i, \quad \kappa''\vec{e}_i, \quad 0^{n}, \quad 0 \ )_{\mathbb{D}},
\end{array}
$$

where $\tau' := -\theta\tau$, $\widetilde{\omega}' := \omega' + \theta\omega''$ and $\widetilde{\kappa}' := \kappa' + \theta\kappa''$, which are independently and uniformly distributed since $\theta, \omega', \kappa' \xleftarrow{\mathsf{U}} \mathbb{F}_q$ except for the case $\tau = 0$. That is, the joint distribution for Exp. 3-0 and that for Exp. 3-1 are equivalent except with probability $1/q$. □

Lemma 15 *For any adversary $\mathcal{B}$, there is a probabilistic machine $\mathcal{C}$, whose running time is essentially the same as that of $\mathcal{B}$, for any security parameter λ,*
$\left|\left|\mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}1}(\lambda) \to 1\right] - \mathsf{Pr}\left[\mathsf{Exp}_{\mathcal{B}}^{3\text{-}2}(\lambda) \to 1\right]\right| - \mathsf{Adv}_{\mathcal{C}}^{\mathsf{P2}}(\lambda)\right| \leq 2/q$.

Proof. In order to prove Lemma 15, we construct a probabilistic machine $\mathcal{C}$ against Problem 2 using a machine $\mathcal{B}$ distinguishing the experiment $\mathsf{Exp}^{3\text{-}1}_{\mathcal{B}}$ from $\mathsf{Exp}^{3\text{-}2}_{\mathcal{B}}$ as a black box as follows: $\mathcal{C}$ is given a Problem 2 instance, $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$. $\mathcal{C}$ sets

$$
\begin{aligned}
&\boldsymbol{f}_i := \eta_1 \boldsymbol{b}_i + \eta_2 \boldsymbol{e}_i \ \text{ for } i = 1, \ldots, n,\\
&\mathbb{D} := (\boldsymbol{d}_i)_{i=0,\ldots,4n+1} := (\boldsymbol{b}_0, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{3n}, \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_{2n}, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}),\\
&\mathbb{D}^* := (\boldsymbol{d}^*_i)_{i=0,\ldots,4n+1} := (\boldsymbol{b}^*_0, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{b}^*_{3n}, \boldsymbol{b}^*_{n+1}, \ldots, \boldsymbol{b}^*_{2n}, \boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n+1}),\\
&\widehat{\mathbb{D}} := (\boldsymbol{d}_0, \ldots, \boldsymbol{d}_n, \boldsymbol{d}_{3n+1}, \ldots, \boldsymbol{d}_{4n+1}) = (\boldsymbol{b}_0, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{3n}, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}),\\
&\widehat{\mathbb{D}}^* := (\boldsymbol{d}^*_0, \ldots, \boldsymbol{d}^*_n, \boldsymbol{d}^*_{2n+1}, \ldots, \boldsymbol{d}^*_{4n+1}) := (\boldsymbol{b}^*_0, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{b}^*_{3n}, \boldsymbol{b}^*_1, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n+1}),
\end{aligned}
$$

where $\mathcal{C}$ can calculate $\widehat{\mathbb{D}}$ and $\widehat{\mathbb{D}}^*$ from a part of the Problem 2 instance, i.e., $(\widehat{\mathbb{B}}, \mathbb{B}^*)$, while $\mathcal{C}$ cannot calculate a part of basis $\mathbb{D}$, i.e., $(\boldsymbol{d}_{n+1}, \ldots, \boldsymbol{d}_{2n})$, from the Problem 2 instance. $\mathcal{C}$ gives $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n})$ to $\mathcal{B}$, and receives $\beta' \in \{0,1\}$. $\mathcal{C}$ then outputs β'.

Then,

$$
\begin{array}{rcccccccc}
 & & \overbrace{}^{1} & \overbrace{\phantom{\delta\vec{e}_i}}^{n} & \overbrace{}^{n} & \overbrace{}^{n} & \overbrace{\phantom{\delta_0\vec{e}_i}}^{n} & \overbrace{}^{1} & \\
\boldsymbol{h}^*_{0,i} := & (& 0, & \delta\vec{e}_i, & 0^n, & 0^n, & \delta_0\vec{e}_i, & 0 &)_{\mathbb{B}^*}\\
= & (& 0, & 0^n, & 0^n, & \delta\vec{e}_i, & \delta_0\vec{e}_i, & 0 &)_{\mathbb{D}^*}\\
\boldsymbol{h}^*_{1,i} := & (& 0, & \delta\vec{e}_i, & \tau\vec{e}_i, & 0^n, & \delta_0\vec{e}_i, & 0 &)_{\mathbb{B}^*}\\
= & (& 0, & 0^n, & \tau\vec{e}_i, & \delta\vec{e}_i, & \delta_0\vec{e}_i, & 0 &)_{\mathbb{D}^*}\\
\boldsymbol{e}_i := & (& 0, & \omega\vec{e}_i, & \sigma\vec{e}_i, & 0^n, & 0^n, & 0 &)_{\mathbb{B}},\\
= & (& 0, & 0^n, & \sigma\vec{e}_i, & \omega\vec{e}_i, & 0^n, & 0 &)_{\mathbb{D}},\\
\boldsymbol{f}_i := & (& 0, & (\eta_1+\eta_2\omega)\vec{e}_i, & \eta_2\sigma\vec{e}_i, & 0^n, & 0^n, & 0 &)_{\mathbb{B}},\\
= & (& 0, & 0^n, & \eta_2\sigma\vec{e}_i, & (\eta_1+\eta_2\omega)\vec{e}_i, & 0^n, & 0 &)_{\mathbb{D}},
\end{array}
$$

where $\delta, \tau, \omega, \sigma, \eta_1 + \eta_2\omega$ and $\eta_2\sigma$ are independently and uniformly distributed in $\mathbb{F}_q$ since $\delta, \tau, \omega, \sigma, \eta_1, \eta_2 \xleftarrow{\cup} \mathbb{F}_q$ except for the case $\sigma = 0$.

That is, the above $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{D}}, \widehat{\mathbb{D}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n})$ has the same distribution as the output of the generator $\mathcal{G}_1^{\mathsf{Exp\text{-}3}}(1^\lambda, n)$ (resp. $\mathcal{G}_2^{\mathsf{Exp\text{-}3}}(1^\lambda, n)$) when $\beta = 1$ (resp. $\beta = 0$) except with probability $1/q$. This completes the proof of Lemma 15. □

Proof of Lemma 6

Lemma 6. *For any adversary $\mathcal{A}$, there exists a probabilistic machine $\mathcal{B}_1$, whose running time is essentially the same as that of $\mathcal{A}$, such that for any security parameter λ, $|\mathsf{Adv}^{(0')}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(1)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(\lambda)$.*

Proof. In order to prove Lemma 6, we construct a probabilistic machine $\mathcal{B}_1$ against Problem 1 using an adversary $\mathcal{A}$ in a security game (Game 0' or 1) as a black box as follows:

1. $\mathcal{B}_1$ is given a Problem 1 instance, $(\mathsf{param}_{\mathbb{V}}, \mathbb{B}, \widehat{\mathbb{B}}^*, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n})$.
2. $\mathcal{B}_1$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_1$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$ of Game 0' (and 1), where $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1})$ is obtained from the Problem 1 instance.
4. When a key query is issued for vector $\vec{v}$, $\mathcal{B}_1$ answers normal key $\boldsymbol{k}^*$ with Eq. (2), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 1 instance.

5. When $\mathcal{B}_1$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ from $\mathcal{A}$, $\mathcal{B}_1$ computes the challenge ciphertext $(\boldsymbol{c}_1, c_2)$ such that,

$$\boldsymbol{c}_1 := \zeta \boldsymbol{b}_0 + x_1^{(b)} \boldsymbol{e}_{\beta,1} + \textstyle\sum_{i=2}^{n} x_i^{(b)} \boldsymbol{e}_i + \varphi \boldsymbol{b}_{4n+1}, \qquad c_2 := g_T^{\zeta} m^{(b)},$$

where $\zeta, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\{\boldsymbol{b}_i\}_{i=0,4n+1}, \boldsymbol{e}_{\beta,1}, \{\boldsymbol{e}_i\}_{i=2,\ldots,n})$ is a part of the Problem 1 instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_1$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_1$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_1$ outputs $\beta' := 0$.

Claim 1 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_1$ given a Problem 1 instance with $\beta \in \{0,1\}$ is the same as that in Game 0' (resp. Game 1) if $\beta = 0$ (resp. $\beta = 1$).*

Proof. We will consider the distribution of $\boldsymbol{c}_1$.

When $\beta = 0$, ciphertext $\boldsymbol{c}_1$ generated in step 5 is

$$\begin{aligned} \boldsymbol{c}_1 &= \zeta \boldsymbol{b}_0 + x_1^{(b)} \boldsymbol{e}_{0,1} + \textstyle\sum_{i=2}^{n} x_i^{(b)} \boldsymbol{e}_i + \varphi \boldsymbol{b}_{4n+1} = \zeta \boldsymbol{b}_0 + \omega \textstyle\sum_{i=1}^{n} x_i^{(b)} \boldsymbol{b}_i + \gamma \boldsymbol{b}_{4n+1} + \varphi \boldsymbol{b}_{4n+1} \\ &= (\ \zeta,\ \omega \vec{x}^{(b)},\ 0^n,\ 0^n,\ 0^n,\ \varphi')_{\mathbb{B}} \end{aligned}$$

where $\varphi' := \varphi + \gamma, \zeta, \omega \in \mathbb{F}_q$ are uniformly and independently distributed.

When $\beta = 1$, ciphertext $\boldsymbol{c}_1$ generated in step 5 is

$$\begin{aligned} \boldsymbol{c}_1 &= \zeta \boldsymbol{b}_0 + x_1^{(b)} \boldsymbol{e}_{1,1} + \textstyle\sum_{i=2}^{n} x_i^{(b)} \boldsymbol{e}_i + \varphi \boldsymbol{b}_{4n+1} \\ &= \zeta \boldsymbol{b}_0 + \omega \textstyle\sum_{i=1}^{n} x_i^{(b)} \boldsymbol{b}_i + x_1^{(b)} z \boldsymbol{b}_{n+1} + \gamma \boldsymbol{b}_{4n+1} + \varphi \boldsymbol{b}_{4n+1} \\ &= (\ \zeta,\ \omega \vec{x}^{(b)},\ x_1^{(b)} z \vec{e}_1,\ 0^n,\ 0^n,\ \varphi')_{\mathbb{B}} \end{aligned}$$

where $\varphi' := \varphi + \gamma, \zeta, \omega \in \mathbb{F}_q$ are uniformly and independently distributed.

Therefore, the above $\boldsymbol{c}_1$ and $c_2 := g_T^{\zeta} m$ give a challenge ciphertext in Game 0' when $\beta = 0$, and that in Game 1 when $\beta = 1$. □

From Claim 1, $\left|\mathsf{Adv}_{\mathcal{A}}^{(0')}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}_1(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P1}}(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_1(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P1}}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_1}^{\mathsf{P1}}(\lambda)$. This completes the proof of Lemma 6. □

Proof of Lemma 7

Lemma 7. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)| \leq 2/q$.*

Proof.

Case that $h = 1$, i.e., proof for $|\mathsf{Adv}_{\mathcal{A}}^{(1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}1\text{-}1)}(\lambda)| \leq 2/q$:

In order to prove Lemma 7 in this case, we define an intermediate game, Game 1', and will show the equivalence of the distribution of the views of $\mathcal{A}$ in Game 1 and that in Game 1' (Claim 2) and those in Game 2-1-1 and in Game 1' (Claim 3).

Game 1' : Game 1' is the same as Game 1 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega \vec{x}^{(b)},\ \boxed{\vec{r}},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{12}$$

where $\vec{r} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{2n} \setminus \{\vec{0}\}$, and all the other variables are generated as in Game 1.

Claim 2 *The distribution* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ *in Game 1 and that in Game 1' are equivalent except with probability* $1/q$.

Proof. We will consider the distribution in Game 1. We define new (dual orthonormal) bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ below. First, we generate $F \xleftarrow{\cup} GL(2n, \mathbb{F}_q)$, and set

$$\left.\begin{array}{l} \begin{pmatrix} \boldsymbol{d}_{n+1} \\ \vdots \\ \boldsymbol{d}_{3n} \end{pmatrix} := F^{-1} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1} \\ \vdots \\ \boldsymbol{b}_{3n} \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{d}^*_{n+1} \\ \vdots \\ \boldsymbol{d}^*_{3n} \end{pmatrix} := F^{\mathrm{T}} \cdot \begin{pmatrix} \boldsymbol{b}^*_{n+1} \\ \vdots \\ \boldsymbol{b}^*_{3n} \end{pmatrix}, \\ \mathbb{D} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{d}_{n+1}, \ldots, \boldsymbol{d}_{3n}, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}), \\ \mathbb{D}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{d}^*_{n+1}, \ldots, \boldsymbol{d}^*_{3n}, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{d}^*_{4n+1}). \end{array}\right\} \tag{13}$$

Then, $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal bases. Challenge ciphertext $\boldsymbol{c}_1$ is expressed as

$$\boldsymbol{c}_1 \;=\; (\,\zeta,\ \omega\vec{x}^{(b)},\ \overbrace{x_1^{(b)} z\vec{e}_1,\ 0^n}^{2n},\ 0^n,\ \varphi)_{\mathbb{B}} = (\,\zeta,\ \omega\vec{x}^{(b)},\ \overbrace{\vec{r}}^{2n},\ 0^n,\ \varphi)_{\mathbb{D}}, \tag{14}$$

where $\zeta, \omega, z, \varphi \xleftarrow{\cup} \mathbb{F}_q$, and $\vec{r} := (x_1^{(b)} z\vec{e}_1,\ 0^n) \cdot F$. Since $x_1^{(b)} \neq 0$, coefficient vector $(x_1^{(b)} z\vec{e}_1,\ 0^n) \neq \vec{0}$ except for probability $1/q$. Then, vector $\vec{r} := (x_1^{(b)} z\vec{e}_1,\ 0^n) \cdot F$ is uniformly distributed in $\mathbb{F}_q^{2n} \setminus \{\vec{0}\}$ except for probability $1/q$ and independent from all the other variables.

Every queried key $\boldsymbol{k}^*$ in Game 1 is

$$\boldsymbol{k}^* = (\,1,\ \sigma\vec{v},\ 0^n,\ 0^n,\ \vec{\eta},\ 0)_{\mathbb{B}^*} = (\,1,\ \sigma\vec{v},\ 0^n,\ 0^n,\ \vec{\eta},\ 0)_{\mathbb{D}^*}, \tag{15}$$

where $\sigma \xleftarrow{\cup} \mathbb{F}_q$ and $\vec{\eta} \xleftarrow{\cup} \mathbb{F}_q^n$.

In the light of the adversary's view, $(\mathbb{D}, \mathbb{D}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Moreover, since the RHS of Eq. (14) and that of Eq. (12) are the same form, the challenge ciphertext $\boldsymbol{c}_1$ and $c_2 := g_T^{\zeta} m$ in Game 1 can be conceptually changed to that in Game 1' except with probability $1/q$. □

Claim 3 *The distribution* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ *in Game 2-1-1 and that in Game 1' are equivalent except with probability* $1/q$.

Proof. We will consider the distribution in Game 2-1-1. We define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ by Eq. (13). Challenge ciphertext $\boldsymbol{c}_1$ is expressed as

$$\boldsymbol{c}_1 \;=\; (\,\zeta,\ \omega\vec{x}^{(b)},\ \overbrace{\omega'\vec{x}^{(b)}, \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)}}^{2n},\ 0^n,\ \varphi)_{\mathbb{B}} = (\,\zeta,\ \omega\vec{x}^{(b)},\ \overbrace{\vec{r}}^{2n},\ 0^n,\ \varphi)_{\mathbb{D}}, \tag{16}$$

where $\zeta, \omega, \omega', \omega''_0, \omega''_1, \varphi \xleftarrow{\cup} \mathbb{F}_q$, and $\vec{r} := (\omega'\vec{x}^{(b)}, \omega''_0\vec{x}^{(0)} + \omega''_0\vec{x}^{(1)}) \cdot F \in \mathbb{F}_q^{2n}$ Since $(\omega'\vec{x}^{(b)}, \omega''_0\vec{x}^{(0)} + \omega''_0\vec{x}^{(1)}) \neq \vec{0}$ except for negligible probability $1/q$, vector $\vec{r} := (\omega'\vec{x}^{(b)}, \omega''_0\vec{x}^{(0)} + \omega''_0\vec{x}^{(1)}) \cdot F$ is uniformly distributed in $\mathbb{F}_q^{2n} \setminus \{\vec{0}\}$ except for negligible probability $1/q$ and independent from all the other variables.

For queried keys $\boldsymbol{k}^*$, the same as Eq. (15) holds also in Game 2-1-1.

In the light of the adversary's view, $(\mathbb{D}, \mathbb{D}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Moreover, since the RHS of Eq. (16) and that of Eq. (12) are the same form, the challenge ci-

phertext $\boldsymbol{c}_1$ and $c_2 := g_T^{\zeta} m$ in Game 2-1-1 can be conceptually changed to that in Game 1' except with probability $1/q$. □

From Claims 2 and 3, adversary $\mathcal{A}$'s view in Game 1 can be conceptually changed to that in Game 2-1-1 except with probability $2/q$. This completes the proof of Lemma 7 when $h = 1$.

Case that $h \geq 2$, i.e., proof for $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}(h-1)\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda)\right| \leq 2/q$ for $h \geq 2$:

To prove Lemma 7 in this case, we define an intermediate game, Game 2-$(h-1)$-4', and will show the equivalence of the distribution of the views of $\mathcal{A}$ in Game 2-$(h-1)$-4 and that in Game 2-$(h-1)$-4' (Claim 4) and those in Game 2-h-1 and in Game 2-$(h-1)$-4' (Claim 5).

Game 2-$(h-1)$-4' : Game 2-$(h-1)$-4' is the same as Game 2-$(h-1)$-4 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ is:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\vec{r}},\ \omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \tag{17}$$

where $\vec{r} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n \setminus \{\vec{0}\}$, and all the other variables are generated as in Game 2-$(h-1)$-4.

Claim 4 *The distribution* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ *in Game 2-$(h-1)$-4 and that in Game 2-$(h-1)$-4' are equivalent except with probability* $1/q$ *when* $h \geq 2$.

Proof. We will consider the distribution in Game 2-$(h-1)$-4. We define new (dual orthonormal) bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ below. First, we generate $F \xleftarrow{\mathsf{U}} GL(n, \mathbb{F}_q)$, and set

$$\left.\begin{array}{l} \begin{pmatrix} \boldsymbol{d}_{n+1} \\ \vdots \\ \boldsymbol{d}_{2n} \end{pmatrix} := F^{-1} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1} \\ \vdots \\ \boldsymbol{b}_{2n} \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{d}_{n+1}^* \\ \vdots \\ \boldsymbol{d}_{2n}^* \end{pmatrix} := F^{\mathrm{T}} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1}^* \\ \vdots \\ \boldsymbol{b}_{2n}^* \end{pmatrix}, \\ \mathbb{D} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{d}_{n+1}, \ldots, \boldsymbol{d}_{2n}, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{4n+1}), \\ \mathbb{D}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{d}_{n+1}^*, \ldots, \boldsymbol{d}_{2n}^*, \boldsymbol{b}_{2n+1}^*, \ldots, \boldsymbol{d}_{4n+1}^*). \end{array}\right\} \tag{18}$$

Then, $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal bases. Challenge ciphertext $\boldsymbol{c}_1$ is expressed as

$$\begin{aligned} \boldsymbol{c}_1 &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)},\ \omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{B}} \\ &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \vec{r},\ \omega_0''\vec{x}^{(0)} + \omega_1''\vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{D}}, \end{aligned} \tag{19}$$

where $\zeta, \omega, \omega_0', \omega_1', \omega_0'', \omega_1'', \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\vec{r} := (\omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)}) \cdot F$. Since $\omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)} \neq \vec{0}$ except for negligible probability $1/q$, vector $\vec{r} := (\omega_0'\vec{x}^{(0)} + \omega_1'\vec{x}^{(1)}) \cdot F$ is uniformly distributed in $\mathbb{F}_q^n \setminus \{\vec{0}\}$ except for negligible probability $1/q$ and independent from all the other variables.

When $1 \leq j \leq h-1$, the j-th queried key $\boldsymbol{k}^{(j)*}$ is

$$\boldsymbol{k}^{(j)*} = (\ 1,\ \sigma^{(j)}\vec{v}^{(j)},\ 0^n,\ \sigma''^{(j)}\vec{v}^{(j)},\ \vec{\eta}^{(j)},\ 0)_{\mathbb{B}^*} = (\ 1,\ \sigma^{(j)}\vec{v},\ 0^n,\ \sigma''^{(j)}\vec{v}^{(j)},\ \vec{\eta}^{(j)},\ 0)_{\mathbb{D}^*}, \tag{20}$$

where $\sigma^{(j)}, \sigma''^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$. When $h \leq j \leq \nu$, the j-th queried key $\boldsymbol{k}^{(j)*}$ is

$$\boldsymbol{k}^{(j)*} = (\ 1,\ \sigma^{(j)}\vec{v},\ 0^n,\ 0^n,\ \vec{\eta}^{(j)},\ 0)_{\mathbb{B}^*} = (\ 1,\ \sigma^{(j)}\vec{v},\ 0^n,\ 0^n,\ \vec{\eta}^{(j)},\ 0)_{\mathbb{D}^*}, \tag{21}$$

where $\sigma^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ and $\vec{\eta}^{(j)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^n$.

In the light of the adversary's view, $(\mathbb{D}, \mathbb{D}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Moreover, since the RHS of Eq. (19) and that of Eq. (17) are the same form, the challenge ciphertext $\boldsymbol{c}_1$ and $c_2 := g_T^{\zeta} m$ in Game 2-$(h-1)$-4 can be conceptually changed to that in Game 2-$(h-1)$-4' except with probability $1/q$. □

Claim 5 *The distribution* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ *in Game 2-h-1 and that in Game 2-*$(h-1)$*-4' are equivalent except with probability* $1/q$.

Proof. We will consider the distribution in Game 2-h-1. We define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ by Eq. (18). Challenge ciphertext $\boldsymbol{c}_1$ is expressed as

$$\begin{aligned} \boldsymbol{c}_1 &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega'\vec{x}^{(b)}, \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{B}} \\ &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \vec{r}, \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{D}}, \end{aligned} \tag{22}$$

where $\zeta, \omega, \omega', \omega''_0, \omega''_1, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, and $\vec{r}' := \omega'\vec{x}^{(b)} \cdot F$. Since $\omega'\vec{x}^{(b)} \neq \vec{0}$ except for negligible probability $1/q$, vector $\vec{r} := \omega'\vec{x}^{(b)} \cdot F$ is uniformly distributed in $\mathbb{F}_q^n \setminus \{\vec{0}\}$ except for negligible probability $1/q$ and independent from all the other variables.

For queried keys $\boldsymbol{k}^{(j)*}$, the same as Eqs. (20) and (21) hold also in Game 2-h-1.

In the light of the adversary's view, $(\widetilde{\mathbb{D}}, \widetilde{\mathbb{D}}^*)$ is consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Moreover, since the RHS of Eq. (22) and that of Eq. (17) are the same form, the challenge ciphertext $\boldsymbol{c}_1$ and $c_2 := g_T^{\zeta} m$ in Game 2-h-1 can be conceptually changed to that in Game 2-$(h-1)$-4' except with probability $1/q$. □

From Claims 4 and 5, when $h \geq 2$, adversary $\mathcal{A}$'s view in Game 2-$(h-1)$-4 can be conceptually changed to that in Game 2-h-1 except with probability $2/q$.

This completes the proof of Lemma 7. □

Proof of Lemma 8

Lemma 8. *For any adversary* $\mathcal{A}$*, there exists a probabilistic machine* $\mathcal{B}_{2\text{-}1}$*, whose running time is essentially the same as that of* $\mathcal{A}$*, such that for any security parameter* λ, $|\mathsf{Adv}^{(2\text{-}h\text{-}1)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2\text{-}h\text{-}1}}(\lambda)$*, where* $\mathcal{B}_{2\text{-}h\text{-}1}(\cdot) := \mathcal{B}_{2\text{-}1}(h, \cdot)$.

Proof. In order to prove Lemma 8, we construct a probabilistic machine $\mathcal{B}_{2\text{-}1}$ against Problem 2 using an adversary $\mathcal{A}$ in a security game (Game 2-h-1 or 2-h-2) as a black box as follows:

1. $\mathcal{B}_{2\text{-}1}$ is given an integer h and a Problem 2 instance, $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \mathbb{B}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$.
2. $\mathcal{B}_{2\text{-}1}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{2\text{-}1}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}')$ of Game 2-$(h-1)$-4 (and 2-h-1), where $\widehat{\mathbb{B}}' := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1})$ is obtained from the Problem 2 instance.
4. When the ι-th key query is issued for vector $\vec{v} := (v_1, \ldots, v_n)$, $\mathcal{B}_{2\text{-}1}$ answers as follows:
   (a) When $1 \leq \iota \leq h-1$, $\mathcal{B}_{2\text{-}1}$ answers keys of the form (8), that is computed using $\mathbb{B}^*$ of the Problem 2 instance.
   (b) When $\iota = h$, $\mathcal{B}_{2\text{-}1}$ calculates $\boldsymbol{k}^*$ using $(\{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}, \{\boldsymbol{b}^*_i\}_{i=0,3n+1,\ldots,4n})$ of the Problem 2 instance as follows:

$$\vec{\eta} := (\eta_1, \ldots, \eta_n) \xleftarrow{\mathsf{U}} \mathbb{F}_q^n, \quad \boldsymbol{k}^* := \boldsymbol{b}^*_0 + \textstyle\sum_{i=1}^n (v_i \boldsymbol{h}^*_{\beta,i} + \eta_i \boldsymbol{b}^*_{3n+i}).$$

   (c) When $\iota \geq h+1$, $\mathcal{B}_{2\text{-}1}$ answers normal keys of the form (2), that is computed using $\mathbb{B}^*$ of the Problem 2 instance.

5. When $\mathcal{B}_{2\text{-}1}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ from $\mathcal{A}$, $\mathcal{B}_{2\text{-}1}$ computes the challenge ciphertext $(\boldsymbol{c}_1, c_2)$ such that,

$$\boldsymbol{c}_1 := \zeta \boldsymbol{b}_0 + \sum_{i=1}^{n} x_i^{(b)} \boldsymbol{e}_i + \sum_{i=1}^{n} (\omega_0'' x_i^{(0)} + \omega_1'' x_i^{(1)}) \boldsymbol{b}_{2n+i} + \varphi \boldsymbol{b}_{4n+1}, \qquad c_2 := g_T^{\zeta} m^{(b)},$$

where $\omega_0'', \omega_1'', \zeta, \varphi \xleftarrow{\mathsf{U}} \mathbb{F}_q$, $b \xleftarrow{\mathsf{U}} \{0,1\}$, and $(\{\boldsymbol{b}_i\}_{i=0,2n+1,\ldots,3n,4n+1}, \{\boldsymbol{e}_i\}_{i=1,\ldots,n})$ is a part of the Problem 2 instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_{2\text{-}1}$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}1}$ outputs $\beta' := 0$.

Claim 6 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{2\text{-}1}$ given a Problem 2 instance with $\beta \in \{0,1\}$ is the same as that in Game 2-h-1 (resp. Game 2-h-2) if $\beta = 0$ (resp. $\beta = 1$).*

Proof. We will consider the joint distribution of $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$.

Ciphertext $\boldsymbol{c}_1$ generated in step 5 is

$$\begin{aligned}
\boldsymbol{c}_1 &= \zeta \boldsymbol{b}_0 + \sum_{i=1}^{n} x_i^{(b)} \boldsymbol{e}_i + \sum_{i=1}^{n} (\omega_0'' x_i^{(0)} + \omega_1'' x_i^{(1)}) \boldsymbol{b}_{2n+i} + \varphi \boldsymbol{b}_{4n+1} \\
&= \zeta \boldsymbol{b}_0 + \sum_{i=1}^{n} x_i^{(b)} (\omega \boldsymbol{b}_i + \sigma \boldsymbol{b}_{n+i}) + \sum_{i=1}^{n} (\omega_0'' x_i^{(0)} + \omega_1'' x_i^{(1)}) \boldsymbol{b}_{2n+i} + \varphi \boldsymbol{b}_{4n+1} \\
&= (\ \zeta,\ \omega \vec{x}^{(b)},\ \sigma \vec{x}^{(b)},\ \omega_0'' \vec{x}^{(0)} + \omega_1'' \vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{B}}
\end{aligned}$$

where $\zeta, \omega, \sigma, \omega_0'', \omega_1'', \varphi \in \mathbb{F}_q$ are uniformly and independently distributed.

When $\beta = 0$, secret key $\boldsymbol{k}^*$ generated in case (b) of step 4 or 6 is

$$\begin{aligned}
\boldsymbol{k}^* &= \boldsymbol{b}_0^* + \sum_{i=1}^{n} (v_i \boldsymbol{h}_{0,i}^* + \eta_i \boldsymbol{b}_{3n+i}^*) = \boldsymbol{b}_0^* + \sum_{i=1}^{n} (v_i (\delta \boldsymbol{b}_i^* + \delta_0 \boldsymbol{b}_{3n+i}^*) + \eta_i \boldsymbol{b}_{3n+i}^*) \\
&= \boldsymbol{b}_0^* + \delta \sum_{i=1}^{n} v_i \boldsymbol{b}_i^* + \sum_{i=1}^{n} (v_i \delta_0 + \eta_i) \boldsymbol{b}_{3n+i}^* \\
&= (\ 1,\ \delta \vec{v},\ 0^n,\ 0^n,\ \vec{\eta}',\ 0\ )_{\mathbb{B}^*}
\end{aligned}$$

where $\vec{\eta}' := (v_1 \delta_0 + \eta_1, \ldots, v_n \delta_0 + \eta_n) \in \mathbb{F}_q^n$ Then, $\delta \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed. Therefore, generated $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$ have the same joint distribution as in Game 2-h-1.

When $\beta = 1$, secret key $\boldsymbol{k}^*$ generated in case (b) of step 4 or 6 is

$$\begin{aligned}
\boldsymbol{k}^* &= \boldsymbol{b}_0^* + \sum_{i=1}^{n} (v_i \boldsymbol{h}_{1,i}^* + \eta_i \boldsymbol{b}_{3n+i}^*) = \boldsymbol{b}_0^* + \sum_{i=1}^{n} (v_i (\delta \boldsymbol{b}_i^* + \tau \boldsymbol{b}_{n+i}^* + \delta_0 \boldsymbol{b}_{3n+i}^*) + \eta_i \boldsymbol{b}_{3n+i}^*) \\
&= \boldsymbol{b}_0^* + \delta \sum_{i=1}^{n} v_i \boldsymbol{b}_i^* + \tau \sum_{i=1}^{n} v_i \boldsymbol{b}_{n+i}^* + \sum_{i=1}^{n} (v_i \delta_0 + \eta_i) \boldsymbol{b}_{3n+i}^* \\
&= (\ 1,\ \delta \vec{v},\ \tau \vec{v},\ 0^n,\ \vec{\eta}',\ 0\ )_{\mathbb{B}^*}
\end{aligned}$$

where $\vec{\eta}' := (v_1 \delta_0 + \eta_1, \ldots, v_n \delta_0 + \eta_n) \in \mathbb{F}_q^n$ Then, $\delta \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed. Therefore, generated $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$ have the same joint distribution as in Game 2-h-2. □

From Claim 6, $\left|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}1)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}2)}(\lambda)\right| = \left|\mathsf{Pr}\left[\mathcal{B}_{2\text{-}h\text{-}1}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P}2}(1^\lambda, n)\right] - \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h\text{-}1}(1^\lambda, \varrho) \to 1 \;\middle|\; \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P}2}(1^\lambda, n)\right]\right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}1}}^{\mathsf{P}2}(\lambda)$. This completes the proof of Lemma 8. □

Proof of Lemma 9

Lemma 9. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}^{(2\text{-}h\text{-}2)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda)| \leq 8/q$.*

Proof. To prove Lemma 9, we will show distribution $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ in Game 2-h-2 and that in Game 2-h-3 are equivalent. For that purpose, we define an intermediate game, Game 2-h-2', as

Game 2-h-2' ($h = 1, \ldots, \nu$) : Game 2-h-2' is the same as Game 2-h-2 except that $\boldsymbol{c}_1$ of the challenge ciphertext for (challenge plaintexts $m := m^{(0)} = m^{(1)}$ and) vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ and the reply to the h-th key query for $\vec{v}$, $\boldsymbol{k}^*$, are:

$$\boldsymbol{c}_1 := (\ \zeta,\ \omega\vec{x}^{(b)},\ \boxed{\vec{r}},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}}, \quad \boldsymbol{k}^* := (\ 1,\ \sigma\vec{v},\ \boxed{\vec{w}},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*},$$

where, if $\vec{x}^{(0)} \cdot \vec{v} = \vec{x}^{(1)} \cdot \vec{v} = 0$, then $(\vec{r}, \vec{w}) \xleftarrow{\cup} W_0 := \{(\vec{r}, \vec{w}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \mid \vec{r} \cdot \vec{w} = 0\}$, and if $\vec{x}^{(0)} \cdot \vec{v} \neq 0$ and $\vec{x}^{(1)} \cdot \vec{v} \neq 0$, then $(\vec{r}, \vec{w}) \xleftarrow{\cup} \mathbb{F}_q^n \times \mathbb{F}_q^n \setminus W_0$, and and all the other variables are generated as in Game 2-h-2.

Claim 7 *The distribution $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ in Game 2-h-2 and that in Game 2-h-2' are equivalent except with probability $4/q$.*

Proof. We will consider the distribution in Game 2-h-2. We define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$. First, we generate matrix $U \xleftarrow{\cup} GL(n, \mathbb{F}_q)$, and set

$$\left.\begin{array}{l} \begin{pmatrix} \boldsymbol{d}_{n+1} \\ \vdots \\ \boldsymbol{d}_{2n} \end{pmatrix} := U^{-1} \cdot \begin{pmatrix} \boldsymbol{b}_{n+1} \\ \vdots \\ \boldsymbol{b}_{2n} \end{pmatrix}, \quad \begin{pmatrix} \boldsymbol{d}^*_{n+1} \\ \vdots \\ \boldsymbol{d}^*_{2n} \end{pmatrix} := U^{\mathrm{T}} \cdot \begin{pmatrix} \boldsymbol{b}^*_{n+1} \\ \vdots \\ \boldsymbol{b}^*_{2n} \end{pmatrix}, \\ \mathbb{D} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{d}_{n+1}, \ldots, \boldsymbol{d}_{2n}, \boldsymbol{b}_{2n+1}, \ldots, \boldsymbol{b}_{4n+1}), \\ \mathbb{D}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{d}^*_{n+1}, \ldots, \boldsymbol{d}^*_{2n}, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{d}^*_{4n+1}). \end{array}\right\} \tag{23}$$

We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$.

The h-th queried key and challenge ciphertext $(\boldsymbol{k}^{(h)*}, \boldsymbol{c}_1, c_2)$ in Game 2-h-2 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as

$$\begin{aligned} \boldsymbol{k}^{(h)*} &= (\ 1,\ \sigma\vec{v},\ \sigma'\vec{v},\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{B}^*} = (\ 1,\ \sigma\vec{v},\ \sigma'\vec{v}Z,\ 0^n,\ \vec{\eta},\ 0\ )_{\mathbb{D}^*}, \qquad (24) \\ \boldsymbol{c}_1 &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega'\vec{x}^{(b)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}} \\ &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega'\vec{x}^{(b)}U,\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{D}}, \\ c_2 &= g_T^{\zeta} m, \qquad (25) \end{aligned}$$

where $Z := (U^{-1})^{\mathrm{T}}$.

From Lemma 5, if $\vec{x}^{(0)} \cdot \vec{v} \neq 0$ and $\vec{x}^{(1)} \cdot \vec{v} \neq 0$, the pair of coefficients $(\omega'\vec{x}^{(b)}U, \sigma'\vec{v}Z)$ are uniformly distributed in $\mathbb{F}_q^n \times \mathbb{F}_q^n \setminus W_0$ and independent from all the other variables except for the case $\omega' = 0$ or $\sigma' = 0$, i.e., except with probability $2/q$.

Also, from Lemma 5, if $\vec{x}^{(0)} \cdot \vec{v} = \vec{x}^{(1)} \cdot \vec{v} = 0$, the pair of coefficients $(\omega'\vec{x}^{(b)}U, \sigma'\vec{v}Z)$ are uniformly distributed in W_0 and independent from all the other variables except for the case $\omega' = 0$ or $\sigma' = 0$, i.e., except with probability $2/q$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$ and the answered keys $\{\boldsymbol{k}^{(j)*}\}_{j \neq h}$. Therefore, by using the above result for the distribution of $(\boldsymbol{k}^{(h)*}, \boldsymbol{c}_1, c_2)$, $\{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}$ and $\boldsymbol{c}_1$ can be expressed as keys and ciphertext in two ways, in Game 2-h-2 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 2-h-2' over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 2-$h$-2 can be conceptually changed to Game 2-h-2' except with probability $4/q$. □

Claim 8 *The distribution* $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ *in Game 2-h-3 and that in Game 2-h-2' are equivalent except with probability* $4/q$.

Proof. Claim 8 is similarly proven as that of Claim 7.

As in Claim 7, we set new bases $(\mathbb{D}, \mathbb{D}^*)$ as in Eq. (23). The h-th queried key $\boldsymbol{k}^{(h)*}$ in Game 2-h-3 is expressed as in Eq. (24) over bases $\mathbb{B}^*$ and $\mathbb{D}^*$, and a part of challenge ciphertext c_2 in Game 2-h-3 is given by Eq. (25). $\boldsymbol{c}_1$ in Game 2-h-3 is expressed over bases $\mathbb{B}$ and $\mathbb{D}$ as

$$\begin{aligned} \boldsymbol{c}_1 &= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}} \\ &= (\ \zeta,\ \omega\vec{x}^{(b)},\ (\omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)})U,\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{D}}. \end{aligned}$$

Using Lemma 5, similar to the proof of Claim 7, we see that $\{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}$ and $\boldsymbol{c}_1$ can be expressed as keys and ciphertext in two ways, in Game 2-h-3 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 2-h-2' over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 2-$h$-3 can be conceptually changed to Game 2-h-2' except with probability $4/q$. □

From Claims 7 and 8, we obtain Lemma 9. □

Proof of Lemma 10

Lemma 10. *For any adversary* $\mathcal{A}$*, there exists a probabilistic machine* $\mathcal{B}_{2\text{-}2}$*, whose running time is essentially the same as that of* $\mathcal{A}$*, such that for any security parameter* λ, $|\mathsf{Adv}^{(2\text{-}h\text{-}3)}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{(2\text{-}h\text{-}4)}_{\mathcal{A}}(\lambda)| \leq \mathsf{Adv}^{\mathsf{P3}}_{\mathcal{B}_{2\text{-}h\text{-}2}}(\lambda)$*, where* $\mathcal{B}_{2\text{-}h\text{-}2}(\cdot) := \mathcal{B}_{2\text{-}2}(h, \cdot)$.

Proof. In order to prove Lemma 10, we construct a probabilistic machine $\mathcal{B}_{2\text{-}2}$ against Problem 3 using an adversary $\mathcal{A}$ in a security game (Game 2-h-3 or 2-h-4) as a black box as follows:

1. $\mathcal{B}_{2\text{-}2}$ is given an integer h and a Problem 3 instance, $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \widehat{\mathbb{B}}^*, \{\boldsymbol{h}^*_{\beta,i}, \boldsymbol{e}_i\}_{i=1,\ldots,n})$.
2. $\mathcal{B}_{2\text{-}2}$ plays a role of the challenger in the security game against adversary $\mathcal{A}$.
3. At the first step of the game, $\mathcal{B}_{2\text{-}2}$ provides $\mathcal{A}$ a public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}')$ of Game 2-h-3 (and 2-h-4), where $\widehat{\mathbb{B}}' := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1})$ is obtained from the Problem 3 instance.
4. When the ι-th key query is issued for vector $\vec{v} := (v_1, \ldots, v_n)$, $\mathcal{B}_{2\text{-}2}$ answers as follows:
   (a) When $1 \leq \iota \leq h-1$, $\mathcal{B}_{2\text{-}2}$ answers keys of the form (8), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 3 instance.
   (b) When $\iota = h$, $\mathcal{B}_{2\text{-}2}$ calculates $\boldsymbol{k}^*$ using $(\{\boldsymbol{h}^*_{\beta,i}\}_{i=1,\ldots,n}, \{\boldsymbol{b}^*_i\}_{i=0,\ldots,n,3n+1,\ldots,4n})$ of the Problem 3 instance as follows:
   $$\sigma \xleftarrow{\cup} \mathbb{F}_q, \quad \vec{\eta} := (\eta_1, \ldots, \eta_n) \xleftarrow{\cup} \mathbb{F}_q^n, \quad \boldsymbol{k}^* := \boldsymbol{b}^*_0 + \textstyle\sum_{i=1}^n (\sigma v_i \boldsymbol{b}^*_i + v_i \boldsymbol{h}^*_{\beta,i} + \eta_i \boldsymbol{b}^*_{3n+i}).$$
   (c) When $\iota \geq h+1$, $\mathcal{B}_{2\text{-}2}$ answers normal keys of the form (2), that is computed using $\widehat{\mathbb{B}}^*$ of the Problem 3 instance.
5. When $\mathcal{B}_{2\text{-}2}$ receives an encryption query with challenge plaintexts $(m^{(0)}, m^{(1)})$ and vectors $(\vec{x}^{(0)}, \vec{x}^{(1)})$ from $\mathcal{A}$, $\mathcal{B}_{2\text{-}2}$ computes the challenge ciphertext $(\boldsymbol{c}_1, c_2)$ such that,
   $$\boldsymbol{c}_1 := \zeta \boldsymbol{b}_0 + \omega \textstyle\sum_{i=1}^n x_i^{(b)} \boldsymbol{b}_i + \sum_{i=1}^n (x_i^{(0)} \boldsymbol{e}_i + x_i^{(1)} \boldsymbol{f}_i) + \varphi \boldsymbol{b}_{4n+1}, \qquad c_2 := g_T^\zeta m^{(b)},$$
   where $\omega, \zeta, \varphi \xleftarrow{\cup} \mathbb{F}_q$, $b \xleftarrow{\cup} \{0,1\}$, and $(\{\boldsymbol{b}_i\}_{i=0,\ldots,n,4n+1}, \{\boldsymbol{e}_i, \boldsymbol{f}_i\}_{i=1,\ldots,n})$ is a part of the Problem 3 instance.

6. When a key query is issued by $\mathcal{A}$ after the encryption query, $\mathcal{B}_{2\text{-}2}$ executes the same procedure as that of step 4.

7. $\mathcal{A}$ finally outputs bit b'. If $b = b'$, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 1$. Otherwise, $\mathcal{B}_{2\text{-}2}$ outputs $\beta' := 0$.

Claim 9 *The distribution of the view of adversary $\mathcal{A}$ in the above-mentioned game simulated by $\mathcal{B}_{2\text{-}2}$ given a Problem 3 instance with $\beta \in \{0,1\}$ is the same as that in Game 2-h-3 (resp. Game 2-h-4) if $\beta = 0$ (resp. $\beta = 1$).*

Proof. We consider the joint distribution of $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$.

Ciphertext $\boldsymbol{c}_1$ generated in step 5 is

$$\begin{aligned}
\boldsymbol{c}_1 &= \zeta \boldsymbol{b}_0 + \omega \textstyle\sum_{i=1}^n x_i^{(b)} \boldsymbol{b}_i + \sum_{i=1}^n (x_i^{(0)} \boldsymbol{e}_i + x_i^{(1)} \boldsymbol{f}_i) + \varphi \boldsymbol{b}_{4n+1} \\
&= \zeta \boldsymbol{b}_0 + \omega \textstyle\sum_{i=1}^n x_i^{(b)} \boldsymbol{b}_i + \sum_{i=1}^n \left(x_i^{(0)} (\omega' \boldsymbol{b}_{n+i} + \omega'' \boldsymbol{b}_{2n+i}) + x_i^{(1)} (\kappa' \boldsymbol{b}_{n+i} + \kappa'' \boldsymbol{b}_{2n+i}) \right) + \varphi \boldsymbol{b}_{4n+1} \\
&= (\ \zeta,\ \omega \vec{x}^{(b)},\ \omega' \vec{x}^{(0)} + \kappa' \vec{x}^{(1)},\ \omega'' \vec{x}^{(0)} + \kappa'' \vec{x}^{(1)},\ 0^n,\ \varphi)_{\mathbb{B}}
\end{aligned}$$

where $\zeta, \omega, \omega', \omega'', \kappa', \kappa'', \varphi \in \mathbb{F}_q$ are uniformly and independently distributed.

When $\beta = 0$, secret key $\boldsymbol{k}^*$ generated in case (b) of step 4 or 6 is

$$\begin{aligned}
\boldsymbol{k}^* &= \boldsymbol{b}_0^* + \textstyle\sum_{i=1}^n (\sigma v_i \boldsymbol{b}_i^* + v_i \boldsymbol{h}_{0,i}^* + \eta_i \boldsymbol{b}_{3n+i}^*) \\
&= \boldsymbol{b}_0^* + \textstyle\sum_{i=1}^n \left(\sigma v_i \boldsymbol{b}_i^* + v_i (\tau \boldsymbol{b}_{n+i}^* + \delta_0 \boldsymbol{b}_{3n+i}^*) + \eta_i \boldsymbol{b}_{3n+i}^* \right) \\
&= \boldsymbol{b}_0^* + \sigma \textstyle\sum_{i=1}^n v_i \boldsymbol{b}_i^* + \tau \sum_{i=1}^n v_i \boldsymbol{b}_{n+i}^* + \sum_{i=1}^n (v_i \delta_0 + \eta_i) \boldsymbol{b}_{3n+i}^* \\
&= (\ 1,\ \sigma \vec{v},\ \tau \vec{v},\ 0^n,\ \vec{\eta}',\ 0\ )_{\mathbb{B}^*}
\end{aligned}$$

where $\vec{\eta}' := (v_1 \delta_0 + \eta_1, \ldots, v_n \delta_0 + \eta_n) \in \mathbb{F}_q^n$ Then, $\sigma, \tau \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed. Therefore, generated $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$ have the same joint distribution as in Game 2-h-3.

When $\beta = 1$, secret key $\boldsymbol{k}^*$ generated in case (b) of step 4 or 6 is

$$\begin{aligned}
\boldsymbol{k}^* &= \boldsymbol{b}_0^* + \textstyle\sum_{i=1}^n (\sigma v_i \boldsymbol{b}_i^* + v_i \boldsymbol{h}_{1,i}^* + \eta_i \boldsymbol{b}_{3n+i}^*) \\
&= \boldsymbol{b}_0^* + \textstyle\sum_{i=1}^n \left(\sigma v_i \boldsymbol{b}_i^* + v_i (\tau \boldsymbol{b}_{2n+i}^* + \delta_0 \boldsymbol{b}_{3n+i}^*) + \eta_i \boldsymbol{b}_{3n+i}^* \right) \\
&= \boldsymbol{b}_0^* + \sigma \textstyle\sum_{i=1}^n v_i \boldsymbol{b}_i^* + \tau \sum_{i=1}^n v_i \boldsymbol{b}_{2n+i}^* + \sum_{i=1}^n (v_i \delta_0 + \eta_i) \boldsymbol{b}_{3n+i}^* \\
&= (\ 1,\ \sigma \vec{v},\ 0^n,\ \tau \vec{v},\ \vec{\eta}',\ 0\ )_{\mathbb{B}^*}
\end{aligned}$$

where $\vec{\eta}' := (v_1 \delta_0 + \eta_1, \ldots, v_n \delta_0 + \eta_n) \in \mathbb{F}_q^n$ Then, $\sigma, \tau \in \mathbb{F}_q$ and $\vec{\eta}' \in \mathbb{F}_q^n$ are uniformly and independently distributed. Therefore, generated $\boldsymbol{c}_1$ and $\boldsymbol{k}^*$ have the same joint distribution as in Game 2-h-4. □

From Claim 9, $\left| \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}3)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(2\text{-}h\text{-}4)}(\lambda) \right| = \left| \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h\text{-}2}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{P3}}(1^\lambda, n) \right] - \mathsf{Pr}\left[\mathcal{B}_{2\text{-}h\text{-}2}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{P3}}(1^\lambda, n) \right] \right| = \mathsf{Adv}_{\mathcal{B}_{2\text{-}h\text{-}2}}^{\mathsf{P3}}(\lambda)$. This completes the proof of Lemma 10. □

Proof of Lemma 11

Lemma 11. *For any adversary $\mathcal{A}$, $|\mathsf{Adv}_{\mathcal{A}}^{(2\text{-}\nu\text{-}4)}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{(3)}(\lambda)| \leq 1/q$.*

Proof. To prove Lemma 11, we will show distribution $(\mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}}, \{\boldsymbol{k}^{(j)*}\}_{j=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ in Game 2-ν-4 and that in Game 3 are equivalent. For that purpose, we define new dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ of $\mathbb{V}$ as follows:

We generate $\theta \xleftarrow{\cup} \mathbb{F}_q$, and set

$$\begin{aligned}
&\boldsymbol{d}_{2n+i} := \boldsymbol{b}_{2n+i} - \theta \boldsymbol{b}_i, \quad \boldsymbol{d}^*_i := \boldsymbol{b}^*_i + \theta \boldsymbol{b}^*_{2n+i} \quad \text{for } i = 1, \ldots, n, \\
&\mathbb{D} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{2n}, \boldsymbol{d}_{2n+1}, \ldots, \boldsymbol{d}_{3n}, \boldsymbol{b}_{3n+1}, \ldots, \boldsymbol{b}_{4n+1}), \\
&\mathbb{D}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{d}^*_{n+1}, \ldots, \boldsymbol{d}^*_{2n}, \boldsymbol{b}^*_{2n+1}, \ldots, \boldsymbol{b}^*_{4n+1}).
\end{aligned}$$

We then easily verify that $\mathbb{D}$ and $\mathbb{D}^*$ are dual orthonormal, and are distributed the same as the original bases, $\mathbb{B}$ and $\mathbb{B}^*$.

Keys and challenge ciphertext $(\{\boldsymbol{k}^{(h)*}\}_{h=1,\ldots,\nu}, \boldsymbol{c}_1, c_2)$ in Game 2-ν-4 are expressed over bases $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ as

$$\begin{aligned}
\boldsymbol{k}^{(h)*} &:= (\ 1,\ \sigma^{(h)}\vec{v}^{(h)},\ 0^n,\ \sigma^{(h)\prime\prime}\vec{v}^{(h)},\ \vec{\eta}^{(h)},\ 0\ )_{\mathbb{B}^*} \\
&= (\ 1,\ \sigma^{(h)}\vec{v}^{(h)},\ 0^n,\ \sigma^{(h)\prime\prime}\vec{v}^{(h)} - \theta\sigma^{(h)}\vec{v}^{(h)},\ \vec{\eta}^{(h)},\ 0\ )_{\mathbb{D}^*} \\
&= (\ 1,\ \sigma^{(h)}\vec{v}^{(h)},\ 0^n,\ \xi^{(h)}\vec{v}^{(h)},\ \vec{\eta}^{(h)},\ 0\ )_{\mathbb{D}^*}, \\
\boldsymbol{c}_1 &:= (\ \zeta,\ \omega\vec{x}^{(b)},\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{B}} \\
&= (\ \zeta,\ \omega\vec{x}^{(b)} + \theta(\omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)}),\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{D}}, \\
&= (\ \zeta,\ \omega_0\vec{x}^{(0)} + \omega_1\vec{x}^{(1)},\ \omega'_0\vec{x}^{(0)} + \omega'_1\vec{x}^{(1)},\ \omega''_0\vec{x}^{(0)} + \omega''_1\vec{x}^{(1)},\ 0^n,\ \varphi\ )_{\mathbb{D}}, \\
c_2 &:= g_T^{\zeta} m,
\end{aligned}$$

where $\omega_b := \omega + \theta\omega''_b$, $\omega_{1-b} := \theta\omega''_{1-b}$ and $\xi^{(h)} := \sigma^{(h)\prime\prime} - \theta\sigma^{(h)} \in \mathbb{F}_q$ are uniformly, independently (from other variables) distributed since $\omega, \theta, \sigma^{(h)\prime\prime} \xleftarrow{\cup} \mathbb{F}_q$, except for the case $\omega''_{1-b} = 0$, i.e., except with probability $1/q$.

In the light of the adversary's view, both $(\mathbb{B}, \mathbb{B}^*)$ and $(\mathbb{D}, \mathbb{D}^*)$ are consistent with public key $\mathsf{pk} := (1^\lambda, \mathsf{param}_{\mathbb{V}}, \widehat{\mathbb{B}})$. Therefore, $\{\boldsymbol{k}^{(h)*}\}_{h=1,\ldots,\nu}$ and $\boldsymbol{c}_1$ above can be expressed as keys and ciphertext in two ways, in Game 2-ν-4 over bases $(\mathbb{B}, \mathbb{B}^*)$ and in Game 3 over bases $(\mathbb{D}, \mathbb{D}^*)$. Thus, Game 2-$\nu$-4 can be conceptually changed to Game 3. □